Federal Office
for Information Security

BSI Technical Guideline 03125
Preservation of Evidence of Cryptographically Signed Documents

Designation	TR-ESOR – Preservation of Evidence of Cryptographically Signed Documents
Abbreviation	BSI TR-ESOR - 03125
Version	1.2.2(on base of the eIDAS-Regulation and ETSI Preservation Standards)
Date	02.07.2019

Federal Office for Information Security
P.O.B. 20 03 63
D-53133 Bonn (Germany)
Phone: +49 228 99 9582-0
E-mail: tresor@bsi.bund.de
Internet: https://www.bsi.bund.de

Foreword by the President

They say that paper is patient. Furthermore, it has many other positive characteristics that are quite tangible. Paper, though, is no longer en vogue: companies, public administration and the judiciary have been continuously increasing the level of digitisation of their business processes and, therefore, storing documents in a digital format for quite some time. The substitution of the typical — even proverbial mountains of paper with electronic documents — not only influences communication and workflow management, but undoubtedly also has far-reaching consequences for the archiving of electronic documents.

The physical nature of paper documents means that they have characteristics that electronic documents do not have per se. Without helpful devices, electronic documents can neither be perceived nor read, nor do they offer clues about their integrity and authenticity. These characteristics regarding the probative value are of utmost importance, though. It is absolutely necessary to take them into account during the migration from paper to electronic data formats. For the long-term preservation of evidence of signed electronic documents, the maintenance of readability and completeness and in particular proof of the integrity and authenticity are indispensable and shall be created and preserved for a long term with technical and organisational measures – at a minimum for the duration of the statutory period of retention.

As a matter of fact, there is already a range of national and international specifications or standards for electronic processing and storage systems. For example, the American Aeronautics and Space Administration (NASA), the European DLM forum and the LTANS working group of the IETF have so far worked on this matter. In Germany the joint project promoted by the Federal Ministry of Economics and Technology (BMWi), "ArchiSig", detailed the legal requirements with regard to the storage of electronically signed documents. These regulations for storage apply in most cases only to certain industries, though, or relate to concrete individual questions and, as a rule, specify few detailed requirements for the preservation of evidence of electronically signed documents as a whole.

The "Technical Guideline for the Preservation of Evidence of Cryptographically Signed Documents (TR-ESOR)" presented in this document thus specifies cross-application requirements and criteria in a modular overall concept for the long-term preservation of evidence of cryptographically signed documents in the context of their storage on the basis of the “Regulation (EU) No 910/2014 of the European Parliament and of the council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC” [(EU)910/2014], the underlying Commission Implementing Decisions and the German law for implementing the “Regulation (EU) No 910/2014 of the European Parliament and of the council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC” [(EU)910/2014] (eIDAS-Durchführungsgesetz **[eIDAS-DG]**)” with the Trust Service Act **(**Vertrauensdienstegesetz **[VDG]**) as article 1 and further existing legal and technical standards as well as national and international experience.

The goal of the TR-ESOR Guideline is to assist in the process of choosing and using suitable security measures for the preservation of evidence of signed electronic documents over long periods of time. Functional and security-related minimum requirements will be defined on the basis of a manufacturer- and product-independent Reference Architecture pursuant to which systems, components, interfaces, and their interaction can be designed, evaluated and put into service for the preservation of evidence.

After all, paper is not just patient, it is reliable. Today, we can still read centuries-old paper documents without any problems. It is well known that such permanence cannot be achieved with electronically readable data carriers. For six centuries, paper was the most important data medium, or more accurately: knowledge medium. Thus, beyond any legal requirements, our task is to make the digital knowledge of our time usable for future generations.

Bonn, July 2019

Arne Schönbohm, President of the BSI

Table of Contents

List of Figures

List of Tables

1. Preliminary remarks

Chapter 1 contains information on the labelling of this Technical Guideline (German: Technische Richtlinie, TR), the body responsible for this subject matter, the version management, the change management and the updating of this Technical Guideline.

1.1 Title

This Technical Guideline bears the title "Technical Guideline for the Preservation of Evidence of Cryptographically Signed Documents (TR-ESOR)".

1.2 Designation

This Technical Guideline is designated as "BSI TR-03125".

1.3 Body responsible for the subject matter

The Federal Office for Information Security (BSI) is responsible for drafting and maintaining this Technical Guideline.

Address: Federal Office for Information Security (BSI)
P.O.B. 20 03 63
D-53133 Bonn (Germany)
Phone: +49 228 99 9582-0
E-mail: tresor@bsi.bund.de
Internet: https://www.bsi.bund.de

1.4 Version management

This Technical Guideline consists of this document and additional separate normative annexes (in this respect, see chapter 10). Furthermore, there will be additional annexes with the corresponding evaluation specifications for the necessary conformity evaluations.

The currently valid parts of this Technical Guideline are:

Part of the Technical Guideline	Version	Date (YYYY-MM-DD)	Notes
Main Document (this document)	1.2.2	2019-07-02	new
Annex TR-ESOR-M.1 ArchiSafe-Module	1.2.2	2019-07-02	new
Annex TR-ESOR-M.2 Cryptographic-Module	1.2.2	2019-07-02	new
Annex TR-ESOR-M.3 ArchiSig-Module			

Part of the Technical Guideline	Version	Date (YYYY-MM-DD)	Notes
Annex TR-ESOR-S Interface Specifications	1.2.1	2018-09-01	Annex S V1.2.1 is historical, is replaced by Annex E V1.2.2 and will in V1.2.2 and higher no longer upgraded further on.
Annex TR-ESOR-E Concretisation of the Interfaces on the Basis of the eCard-API-Framework	1.2.2	2019-07-02	new
Annex TR-ESOR-F Formats	1.2.2	2019-07-02	new
Annex TR-ESOR-B German Federal Agency Profiling	1.2.1	2018-09-01	Annex C.1 V1.2.1 is also part of TR-ESOR V1.2.2
Annex TR-ESOR-C.1 Conformity Test Specification (Level 1 - Functional Conformity)	1.2.1	2018-09-01	Annex C.2 V1.2.1 is also part of TR-ESOR V1.2.2
Annex TR-ESOR-C.2 Conformity Test Specification (Level 2 - Technical Conformity)	1.2.1	2018-09-01	Annex C.3 V1.2.1 is also part of TR-ESOR V1.2.2
Annex TR-ESOR-C.3 Conformity Test Specification (Level 3 - Conformity with the German Federal Agency Profiling)	1.2.2	2019-07-02	new
Annex TR-ESOR-ERS Evidence Record Profiling pursuant to RFC 4998 and RFC 6283	1.2.1	2018-09-01	Annex VR V1.2.1 is also part of TR-ESOR V1.2.1
Annex TR-ESOR-VR Verification Reports for Selected Data Structures			
Annex XBDP XAIP Profiling with **XB**ARCH, X**D**OMEA and **P**REMIS	1.2.2	2019-07-02	new

1.5 Change management / updating

The Technical Guideline and its normative annexes are subject to continuous improvement and adjustments to new requirements. The updates shall be made in an orderly manner, i.e. the adjusted versions of the Technical Guideline shall be authorised in a formal act.

Formally, authorised versions or patches will be published on the BSI website. Publication is done in a regulated manner.

1.6 Publication

The currently valid versions will be offered for download on the BSI's TR-ESOR websites.

The versions will be listed on the table of changes available on BSI's TR-ESOR websites with a description of the addition or change and the respective date.

1.7 Conventions

The requirements and recommendations specified in this Technical Guideline for systems for the preservation of evidence of cryptographically signed documents are labelled in an unambiguous manner. In doing so, the following applies:

- The requirement will get its own unique ID in the form **(Ax.y-z)**, in which case
  x is the respective main chapter,
  y is the respective sub-chapter and
  z is a sequential number within the sub-chapter.

Pursuant to **[RFC2119]**, each requirement will be explicitly specified as obligatory, recommended or optional.

Obligatory requirements (SHALL requirements) are requirements the implementation of which is absolutely necessary. Within the text, they are marked using the words shall / is (are) / shall only / shall not.

Recommended requirements (SHOULD requirements) should be implemented. Within the text, they are marked using the words should / recommended.

Optional requirements (MAY requirements) may be implemented or not. Within the text, they are marked using the words can / could / may.

In some cases, it is necessary to use slightly modified variations of the words mentioned above. However, the meaning of SHALL, SHOULD and MAY is always clear and the definitions above apply in the corresponding manner. Additional explanations on these labelling terms can be found in chapter 9.3.

Under the term "documents" usually used in this Technical Guideline, unless explicitly used with another meaning, record, data and documents are subsumed.

2. Area of application

The primary areas of application of this Technical Guideline are the Federal Agencies in Germany in the scope of the statutory duties to retain certain documents. Furthermore, the Technical Guideline has the character of a recommendation.

3. General information and overview

In this chapter, the layout and contents of the Technical Guideline as well as the primary goals and challenges for long-term preservation of evidence in the context of storing electronic documents are explained.

3.1 Layout and contents of the Technical Guideline

The Technical Guideline consists of this Main Document and a range of supplementary annexes, in which the individual aspects are specified and explained in more detail.

In this Main Document, the statutory framework conditions and standards, the basic goals and requirements and the processes and functions to be mapped are described. Requirements for the setup as well as the system technology and a recommended system architecture (Reference Architecture) will be derived from this. Additionally, the security objectives and security measures for such a system are described. The conclusion describes the scope and contents of a conformity evaluation of technical product solutions based on the requirements defined in this Technical Guideline.

Furthermore, chapter 10 in this Main Document includes an overview of the annexes published and planned. In these supplementary annexes, the requirements defined in this Main Document will be specified and explained based on a functional platform- and product-neutral Reference Architecture described in chapter 6.5.

The description of the goals and requirements is strictly product- and manufacturer-neutral and is oriented solely to the corresponding legal requirements for the preservation of evidence of cryptographically signed electronic documents.

3.2 Subject of the research and definition of terms

The permanent and unchangeable storage (saving) of electronic documents and other data is generally referred to as "**electronic archiving**" in common language usage in the information technology field. From an information technology perspective, the time horizon described using the term "permanent" is a period of time not specified in more detail in which significant, but generally hardly foreseeable technical or technological changes could take place that, among other things, could result that the information technology systems, with which the documents were originally written, created and saved, are no longer available. In the meantime, the term "**electronic (digital) long-term storage**" is used to highlight the difference compared to a short-term "**living records filling**" or backup.[1]

From a legal perspective, the term **"archiving"** in Germany is specified by and reserved for the Federal and State Archiving Laws and shall therefore be differentiated from storage over a limited period of time.

In a legally correct sense, archiving solely concerns government documents and refers to how the documents of a government agency are to be sorted out and preserved by a competent governmental facility (Federal Archive) for an unlimited period of time as soon as they are no longer needed for the purposes of that agency (see §§ 1, 3, 5 and 8 German Federal Archiving Law **[BarchG]**).

Those documents contain a so called permanent value for permanent protection.

The appraisal and decision of the permanent value lies in the responsibility of the respective archive only. All authorities in the area of responsibility have the obligation to offer any record which they don`t need any more for their business during the disposition process, typically at the end of the retention periods, to the respective archive for the archival appraisal.

[1] The definitions of the terms "living records filling", "long-term storage" and "archival storage" can be found in the eGovernment-Masterplan 2010 of the Land of Lower Saxony on page 26; see http://www.niedersachsen.de/download/45825.

A deletion is, independent from deletion obligation e.g. based on data privacy regulations, typically only possible after a negative archival appraisal decision. All records that are of archival value have to be transferred to the respective archive in an adjusted form for permanent storage.

If the responsible archive contains intermediate archive the concerned authorities can transfer their records to it before the retention time expired. In this case the compliant long-term preservation during the retention time will be executed in the technical responsibility of the archive. The data owners are still the concerned authorities where the records were created until the retention time expires. The tasks regarding the preservation of evidence of cryptographically signed records in the intermediate archive are in scope of this Technical Guideline.

However, the questions and requirements with no regard to preservation of evidence of cryptographically signed documents are not subject of this Technical Guideline.

Furthermore, this Technical Guideline does not formulate general requirements for the storage and saving of all kinds of electronic records, either.

The subject and goal of this Technical Guideline is the **preservation of cryptographically signed documents** in the context of their storage. It is worth mentioning here that the necessity of such preservation of evidence is not present per se, but rather should correspond to specific requirements.

With regard to the term "preservation of evidence", it must be noted that each electronic document can be used as evidence pursuant to § 286 of the German Code of Civil Procedure **[ZPO]** in the scope of the free consideration of evidence. Prima facie evidence pursuant to § 371a **[ZPO]** is to be differentiated from this.

In order to furnish this prima facie evidence, if applicable, special measures (for example, the validation of qualified electronic signature pursuant to Article 32 of **[eIDAS]** or in some circumstances a signature or seal or time-stamp renewal pursuant to § 15 of the German Trust Service Act **(**Vertrauensdienstegesetz **[VDG]**) or [**ETSI SR 019 510], [ETSI TS 119 511]** and **[ETSI TS 119 512]** are necessary pursuant to the current legal situation. If these measures are neglected, then a document does not lose all of its probative value, but rather merely the special probative value pursuant to § 371a **[ZPO]**.

The term "preservation of evidence" in this Technical Guideline is to be understood and interpreted in this sense.

NOTICE: *In the following text the term "**digital signature"** covers "advanced electronic signatures" pursuant to **[eIDAS, Article 3(11)],** "qualified electronic signatures" pursuant to **[eIDAS, Article 3(12)]**, "advanced electronic seals" pursuant to **[eIDAS, Article 3(26)]** and "qualified electronic seals" pursuant to **[eIDAS, Article 3(27)]**. Insofar, the term "digital signed document" covers as well documents signed by advanced electronic signatures or seals as documents signed by qualified electronic signatures or seals.*

*In this TR the term "**cryptographic signed documents**" covers not only qualified signed documents pursuant to **[eIDAS, Article 3(12)]** or qualified sealed documents pursuant to **[eIDAS, Article 3(27)]** or qualified time-stamped documents pursuant to **[eIDAS, Article 3(34)]** (within the meaning of the eIDAS regulation)) but also documents with advanced electronic signatures pursuant to **[eIDAS, Article 3(11)]** or with advanced electronic seals pursuant to **[eIDAS, Article 3(26)]** or with electronic time-stamps pursuant to **[eIDAS, Article 3(33)]**, as they are often used in the internal communication of public authorities. What is not meant here are documents with simple signatures or seals based on other (e.g. non-cryptographic) technologies.*

Digital Signatures in the sense of

- the "**Regulation (EU) No 910/2014 o**f the European Parliament and of the council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC" from July 23th 2014 **[(EU)910/2014]**, which is commonly known as "**eIDAS-Regulation**" and

- the "**Law for Implementing the "Regulation (EU) No 910/2014** of the European Parliament and of the council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC" **[(EU)910/2014]** (eIDAS-Durchführungsgesetz **[eIDAS-DG]**),
- especially the **Trust Service Act (**Vertrauensdienstegesetz **[VDG]**) as article 1 of the eIDAS-Durchführungsgesetz **[eIDAS-DG]**

serve to prove the authenticity and integrity of electronic documents and data.

"Electronic time-stamp' means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time" **[eIDAS, Article 3(33)].**

A qualified electronic time-stamp pursuant to **[eIDAS, Article 3(34)] "**shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound."**[eIDAS, Article 41 (2)].**

Therefore, qualified electronic time-stamps establish the evidence of integrity and of proof of existence at a specific date/time.

However, the conclusiveness of these digital signatures or electronic time-stamps can be reduced over the course of time, for example because the cryptographic procedures used could lose their suitability as a security measure. To maintain the full conclusiveness and the ability to use facilitated evidence (see above), additional measures are thus necessary in addition to the unchangeable storage of the documents and digital signatures or electronic time-stamps in many cases. These measures will be defined and specified in this Technical Guideline.

The Technical Guideline assumes the use of self-contained archival information package2 on base of stable data formats for which the intended retention periods are appropriate; the transformation of cryptographically signed documents into other data formats will not be considered here.3

NOTICE: *In this TR-ESOR- Version 1.2.2, the word "XAIP" means in all TR-ESOR- Annexes with the exception of this main document HD, of Annex F and Annex E the following possibilities:*

a) the XML-based archival information package "XAIP" pursuant to ***[TR-ESOR V1.2.2, Annex F, clause 3.1]*** *as well as*

b) the logical XAIP "LXAIP" pursuant to ***[TR-ESOR V1.2.2, Annex F, clause 3.2]*** *as well as*

c) the "ASiC-AIP" pursuant to ***[TR-ESOR V1.2.2, Annex F, clause 3.3]*** *on base of* ***[ETSI EN 319162-1].***

In TR-ESOR Version 1.2.2, the main document HD, the Annex F and E differentiate in detail between XAIP, LXAIP und ASiC-AIP.

A suitable IT component for securing the conclusiveness is referred to as "**TR-ESOR-Middleware**" in this Technical Guideline. Such a component includes neither the custom applications nor the actual storage or archiving systems, but rather bundles the necessary functions for the cryptographic preservation of evidence. A TR-ESOR-Middleware that complies with this Technical Guideline is capable of maintaining the probative value of signed and unsigned electronic data or documents for the entire duration of the retention period.

Additional important definitions of terms, such as data, document, meta data etc. can be found in chapter 12.

3.3 Overview

The goal of the long-term preservation of evidence of cryptographically signed documents is the possible provision of proof for the duration of the storage that certain digital documents and data (payload data) as well as associated meta data were present at a verifiable point in time and have not been changed

2 See Annex F

3 The TransiDoc project was concerned with the transformation of such documents, see http://www.transidoc.de.

since then (integrity). To the extent required, additional verifiable proof of the issuer (authenticity) of the documents and data stored is to be retained pursuant to the legal requirements.

The goal and challenge of an overall system for saving and preservation of evidence of cryptographically signed documents is to ensure for digital contents and supplemental evidence meta data that

- the availability and readability,
- the integrity (intactness),
- the authenticity (and thus the non-repudiation),
- the negotiability (German Word::Verkehrsfähigkeit) and
- Data protection, data security confidentiality

are guaranteed for the whole retention period.

Such an overall system thus also includes those elements (components) and processes that are used for the creation, saving, indexing, searching, administration, reading and long-term storage with integrity of the data to be saved even if these elements (components) and processes are not described in this Technical Guideline. As a rule, these include

- The IT infrastructure included for archiving (Long-Term Storage) (see below)
- The IT applications that archive or work with data and documents.

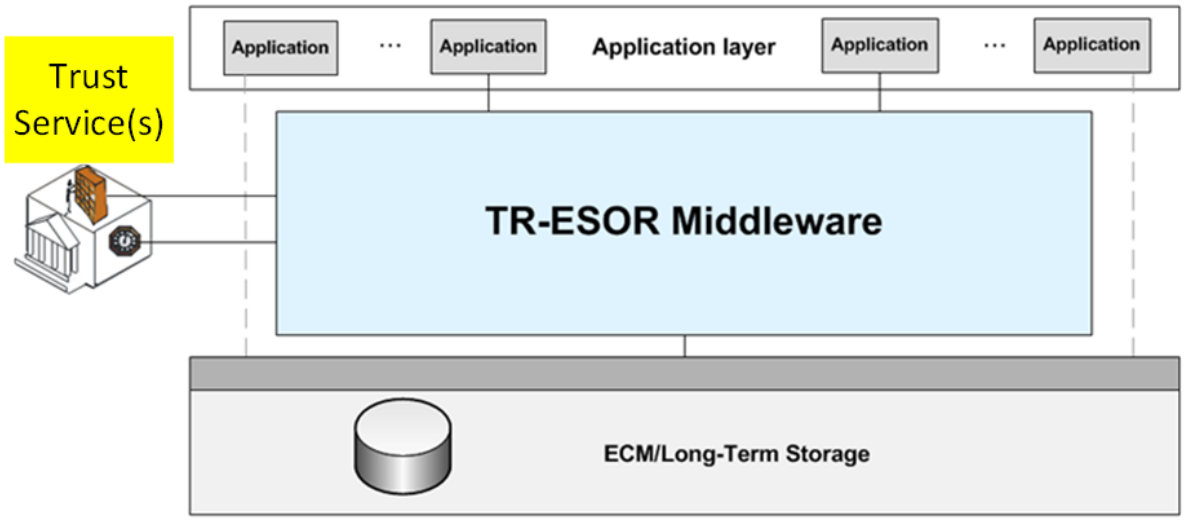


Figure 1: Typical infrastructure for long-term archiving with preservation of evidence

As also depicted in Figure 1, the IT infrastructure used for archiving typically consists of

- an Enterprise Content Management ECM/Long-Term Storage system that includes and manages various storage media used for archiving and which guarantees the reliable and secure access to the storage media for depositing, retrieving, and deleting archived documents and data,
- The Middleware, including the cryptographic components contained therein, that supports the preservation of the probative value of the archived records (documents and data). In this Technical Guideline, this Middleware is referred to as TR-ESOR-Middleware or simply as the Middleware.

The IT applications used for archiving typically include programs for creating, indexing, and managing the documents to be archived, and for researching, displaying, or also deleting data and documents from the archive system. The Technical Guideline is limited to the functions, interfaces and components needed for the preservation of evidence. Additional functions, interfaces and components are allowed provided that they do not compromise the functions for the preservation of evidence or endanger their

security. This is indicated with the dotted lines in Figure 1. However, these additional functions, interfaces and components are not examined here in more detail.

Securing the **availability and readability** of electronic documents cannot be guaranteed by the Middleware that is in the focus of this Technical Guideline; rather, it shall be supported by suitable technical and organisational measures both in the upstream IT applications and in the ECM/Long-Term Storage systems used.

Regardless of the technology, procedures and applications used, the legal representatives are responsible for compliance with the statutory requirements for the long-term preservation of evidence. The main laws and policies are described below.

4. General requirements for storage with preservation of evidence

This Technical Guideline deals with the long-term preservation of evidence of cryptographically signed documents.

NOTICE: *The storage of documents should generally be designed in such a manner that the duties to retain certain documents can at least be fulfilled for the term of the legally defined retention periods.4If the party storing documents wants to design the storage of cryptographically signed documents in such a manner that the conclusiveness of the documents is maintained, then the legal framework conditions5 with regard to this shall be taken into account and the functional requirements shall be defined correspondingly.*

4.1 Federal Archiving Law and the State Archiving Laws

Before destroying them, all federal and state public bodies are legally obliged to offer documents that are no longer needed for carrying out tasks to the Federal or State Archive to be taken over as federal / state archive material (see § 3 and 5**[BArchG]** and the corresponding State Archiving Laws). This duty to offer also applies, of course, to electronic documents.

NOTICE: *Pursuant to § 3 and 5* ***[BArchG]****, all of the documents of federal agencies shall generally be stored; the area-specific regulations pursuant to the German Civil Code* ***[BGB]****, German Commercial Code* ***[HGB]****, etc. do not imply authorisations to delete, but merely indicate minimum legal retention periods. Pursuant to § 3 and 5* ***[BArchG]****, the decision about the permanent or archival value is only in the responsibility of the Federal Archive in consultation with the federal agency making the offer. The criteria of a decision about the "archival value" do not necessarily arise from the reasons under the relevant law for the origin of the documents (compare with § 1* ***[BArchG])****.*

4.2 Legal framework conditions

4.2.1 "Regulation (EU) No 910/2014"[eIDAS] and the German "Law for Implementing the "Regulation (EU) No 910/2014"" as an omnibus law [eIDAS-DG] with the Trust Service Act ([VDG])

Against the background of the experiences gathered with the implementation of the European Signature Directive **[1999/93/EC]** in the different Member States of the European Union and in cross-border scenarios, the European Commission in June 2012 started the legislative procedure **[2012/0146/COD]** and published the "Proposal for a regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market" **[COM(2012)238]**. In 2014 the "Regulation (EU) No 910/2014 of the European Parliament and of the council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC"**[eIDAS]** was finally published, which is commonly known as "eIDAS-Regulation" and which is referenced with **[eIDAS]**.

NOTICE: *As an EU-Regulation, the eIDAS-Regulation* ***[eIDAS]*** *is an immediately applicable law in all 28 EU-Member States as well as in the* ***European Economic Area****.*

As a consequence, in Germany the **German Signature Law [SigG]** was repealed in 2017 by Article 12 of the **"Law for Implementing the "Regulation (EU) No 910/2014""** of 23 July 2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC**"** (German: eIDAS-Durchführungsgesetz **[eIDAS-DG]**)". The **"Law for Implementing the "Regulation (EU) No**

4 In this respect, see § 18 Paragraph 1 Clause 2 of the Directive on the Processing and Management of Records in Federal Ministries (**[RegR]**), also referred to as Registry Directive.

5 For example, see §§ 110a-d German Social Security Code IV.

910/2014" is an omnibus law (German: Artikel Gesetz), whose main important core part is the Article 1 of the **Trust Service Act (**Vertrauensdienstegesetz **[VDG]**). As with the termination of the **German Signature Law** the legal basis of the **German Signature Ordinance Law [SigV]** finished, it is also repealed.

Until this date, pursuant to the **German Signature Law [SigG],** there existed besides qualified electronic timestamps only the following types of electronic signatures: (simple) electronic signatures pursuant to **[SigG, § 2(1)]**, advanced electronic signatures pursuant to **[SigG, § 2(2)]**, qualified elektronic signatures **[SigG, § 2(3)]** and qualified electronic signatures with **vendor accreditation [SigG, § 15]** and qualified electronic signatures with **manufacturer's declaration [SigG, § 17]**.a

The eIDAS-Regulation **[eIDAS]** specifies beside (simple) electronic signatures **[eIDAS, Article 3(10)]** advanced signatures **[eIDAS, Article 3(11)] a**nd qualified signatures **[eIDAS, Article 3(12)]** and furthermore**,** electronic time-stamps **[eIDAS, Article 3(33)] a**nd qualified electronic time-stamps **[eIDAS, Article 3(34)]**.

Qualified electronic time-stamps meet the requirements laid down in **[eIDAS, Article 42] a**nd are provided with an advanced electronic signature of a qualified trust service provider or with an advanced electronic seal of a qualified trust service provider or by an equivalent method.

In addition, as a counterpart to electronic signatures for natural persons, the eIDAS-Regulation **[eIDAS]** introduces **electronic seals**, which also may be used by organisations (legal persons) und defines beside simple seals **[eIDAS, Article 3(25)]** also advanced seals **[eIDAS, Article 3(26)] a**nd qualified seals **[eIDAS, Articl 3(27)].** Furthermore, new Trust Services are introduced in **[eIDAS]** such as for example electronic registered delivery services, certificate services for website authentication and preservation service.

Pursuant to **[eIDAS]** there exist only two classes of Trust Service Providers, non-qualified Trust Service Provides **[eIDAS, Article 3(19)] a**nd qualified Trust Service Providers **[eIDAS, Article 3(20)]**.

Pursuant to the Signature Law **[SigG, § 5, Section 6]** the certification service provider shall convince itself in an appropriate way, that the applicant possesses the associated secure electronic signature creation device. In contrary to this, pursuant to the eIDAS-Regulation **[eIDAS, Annex II Section 3],** the generating or managing of electronic signature creation data on behalf of the signatory (of the responsible person) may be possible but may only be done by a qualified trust service provider.

Further details concerning the legal framework of the eIDAS-Regulation [eIDAS] will be published in short time under the link:
https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/ElektronischeSignatur/RechtlRahmenbedingungen/rechtlrahmenbedingungen_node.html.

Pursuant to German procedural law, an electronic document has a special probative value comparable to a document in written form if it bears a qualified electronic signature. Pursuant to §371a Paragraph 1 **[ZPO]**, the authenticity of a document is assumed if the **successful validation of a qualified electronic signature pursuant to [eIDAS, Article 32]** is presented, provided that there are no serious doubts that the statement was given by the signatory.[6]

Furthermore, the assumption of authenticity pursuant to § 437 Paragraph 1 **[ZPO]** applies to qualified signed public electronic documents, signed by a public authority, pursuant to § 371a Paragraph 3 Clause 2 **[ZPO]** provided that the document turns out to be a public document based on its form and contents.

The appearance or assumption of the authenticity of signed electronic documents[7] is based both on the assignment of the document to the responsible person (owner of the signature key) and that the responsible person really has given the statements contained in the document (see § 416 **[ZPO]**). If the document is an official document in the sense of § 415 **[ZPO]**, it even provides full evidence of the content documented.

[6] § 371a Paragraph 1 Clause 2 **[ZPO]**: The appearance of authenticity of a declaration of intent present in electronic form that is verified based on a qualified electronic signature pursuant to **[eIDAS, Article 32]** may only be unsettled by facts that cast serious doubt on the signature key holder having actually expressed their will.

[7] See also [TR-03138 RESISCAN, Annex TR-RESISCAN **[TR-03138-R]**

Pursuant to **[eIDAS]** the following regulations of the probative value (provision relating to evidence of documents) are valid e.g.

1. **[eIDAS, Article 25 Paragraph 2]**: "*A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.*"
2. **[eIDAS, Article 35 Paragraph 2]**: "*A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.*"
3. **[eIDAS, Article 41 Paragraph 2]:** "*A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.*"

The key prerequisite for determining the probative value of a digitally signed or timestamped document is the successful verification of the electronic signatures, seals or time-stamps. For that reason, security measures that are suited to guaranteeing the authenticity and integrity of the digitally signed or timestamped data in the long term, at a minimum for the duration of the statutory periods of retention are necessary in order to secure the probative value of digital signatures or electronic time-stamps. This applies in particular when the documents to be stored will still be needed after the retention period in cryptographically signed form and it is determined that the algorithms and parameters that form the basis of the digital signatures or time-stamps no longer offer sufficient security for the required or desired retention period and thus make it necessary to take new measures for protection of integrity in the sense of § 15 of the **Trust Service Act [VDG]** and of **[ETSI SR 019 510]**, **[ETSI TS 119 511]** and **[ETSI TS 119 512]**.

4.2.1.1 Durable proof of the authenticity of cryptographically signed documents

With regard to securing the authenticity of the data cryptographically signed (signed, sealed or timestamped according to chapter 3.2), it is of utmost importance that it is and remains possible to prove over the long term to whom the electronic signature or seal or time-stamp can be assigned, i.e. it shall be possible to determine the author of the data cryptographically signed in an unambiguous manner.

The necessary precautions for securing the authenticity for the long-term preservation of electronic data are included in the eIDAS-Regulation **[eIDAS, Article 34 or 40]** and in **[ETSI SR 019 510], [ETSI TS 119 511]** and **[ETSI TS 119 512]** and **Trust Service Act [VDG, § 13 und § 15]**.

Thus, in addition the missing precautions shall be developed based on a consideration with regard to security technology and from the requirements with regard to the laws of evidence for a verification of certificates pursuant to the **[eIDAS, Article 24, Annex I, III and IV]** and **[VDG, § 16]**.

The indication of qualified signatures or qualified seals is managed by qualified certificates fulfilling the requirements concerning the mandatory contents pursuant to **[eIDAS-VO, Anhang I]** or **[eIDAS-VO, Anhang III]** and **[VDG, § 12].**Such a certificate is a confirmation of the assignment of a reliably identified signatory or creator of a seal to the signature or seal validation data (verification key) pursuant to **[eIDAS, Annex I]** or **[eIDAS, Annex III]** with which corresponding electronic signature or seal creation data pursuant to **[eIDAS, Article 3(13)]** or **[eIDAS, Article 3(28)]** the corresponding qualified signature or qualified seal was created.

NOTICE: *In the following text* ***signature or seal validation data*** *pursuant to* ***[eIDAS]*** *is also called signature or seal validation key and s****ignature or seal creation data*** *pursuant to* ***[eIDAS]*** *also (private) signature or seal key.*

If in case of a qualified electronic signature the requirements pursuant to **[eIDAS, Article 32]** or in case of a qualified electronic seal the requirements pursuant to **[eIDAS, Article 40]** are analogously fulfilled , the proof of authenticity can then generally be demonstrated provided that the verification of the certificate pursuant to **[eIDAS, Annex I]** or **[eIDAS, Annex III]** was successful.

Verifiability of the required certificates

It is thus of significance for the long-term proof of the integrity and authenticity of the data signed or sealed, and especially of the electronic time-stamps, that the existence of the certificate and its validity at the time the signature or seal was created remain verifiable **[eIDAS, Point (b) of Article 32(1)]** or **[eIDAS, Article 40]**.

Pursuant to **[eIDAS]**, a necessary prerequisite for the verification of a qualified certificate is that the certificate is available at all. A qualified Trust Service Provider shall keep the qualified certificates issued by it pursuant to **[eIDAS, Point (k) of Article 24(2)]** and **[eIDAS, Article 24(4)]** and **[eIDAS, Annex I** or **Annex III]** verifiable at all times by means of publicly accessible communication channels and also keep them retrievable if the signatory or the creator of the seal agrees **[eIDAS, Point (f) of Article 24(2), Sentence i]**.

The verifiability is based on the presumption that the certificate is available in the certificate directory to be kept by the qualified Trust Service Provider pursuant to **[eIDAS, Point (k) of Article 24(2)]**.

For that reason, a signature or seal validation, also in connection with a time-stamp validation pursuant to **[eIDAS]**, demands beside the fact that the technical validity of the signature or seal can be verified, which means that the verification of whether the signature or seal can be verified correctly cryptographically and whether the signature and the signed data or the seal and sealed data belong together technically, in any case also always an inquiry at the qualified trust service provider about whether the certificate, on which the signature or seal is based, was available, valid and not revoked at the indicated signature or seal creation time. Pursuant to **[eIDAS, Article 24(4)] a**nd **[eIDAS, Point (h) and (i) of Annex I]** or **[eIDAS, Point (h) and (I) of Annex III]**, the qualified trust service provider shall provide this information through publicly accessible communication channels. Because the authenticity of the information shall be verifiable, information provided by the qualified trust service provider is usually furnished with a qualified electronic signature or a qualified electronic seal.

However, these duties of the qualified trust service provider are limited. First of all, the responsible signatory key owner or seal creator may decide pursuant to **[eIDAS, Point (f) of Article 24(2) Sentence I]** that his certificate should not be retrievable. In this case, the qualified trust service provider is not allowed to provide the certificate for retrieval. The signatory or creator of the seal himself shall provide the intended recipient of the data he signed or sealed with the certificate in another way, for example by attaching the certificate to the signature or seal.

On base of the German **Trust Service Act [VDG, § 16] "permanently testable trust services"** are provided**.** This means in detail:

If a qualified trust service provider ends operations, the qualified trust service provider is obligated to ensure that "in case of termination of the service, revocation of the status "qualified" or if an opening of insolvency proceedings is applied and the technical operation will not be continued, *all qualified certificates, issued by this trust service provider, in connection with electronic signatures and seals and certificates in connection with Annex I (g), Annex III (g) and Point (c) of Article 42(1) of the regulation (EU) Nr. 910/2014 including the revocation instruction*

1. can be taken over by another qualified trust service provider or

2. can be taken over by the German Federal Network Agency (BNetzA) in its trust service infrastructure pursuant to Section 5" **[VDG, § 16 Section 1]**. Furthermore, the Federal Network Agency is obliged, "to install, to provide and to actualize permanently a trust service infrastructure for a permanent validation of qualified certificates and qualified electronic time-stamps.[8]

Retention of the required validation data

Based on legal limitation of the permanent verifiability only to qualified electronic certificates and qualified electronic timestamps pursuant to [VDG, § 16 Section 5] the recipient of cryptographically

[8] See § 371a Section 1 Sentence 2 ZPO

signed records may have the obligation or duty to present the certificate together with related verification data by himself if these data are needed for an requested evidence verification[9].

As a rule, the recipient will therefore make the precaution of not only obtaining the cryptographically signed data and digital signature or time-stamp, but also the required certificates and verification information and saving them together with the cryptographically signed data at the latest upon saving them in the electronic ECM/Long-Term Storage if not already upon receipt or issuance of the data signed by using the TR-ESOR-middleware for evidence preservation.[10]

For digital signatures based on a qualified certificate, it is necessary to present and technically verify the following data in order to verify the existence and validity of the certificate at the time the signature or seal was created in a coherent and traceable manner (see **[ARO 07]**, p. 73):

- The user certificate with the certificate chain up to the root certificate,
- A status (OCSP) report[11] from the qualified trust service provider regarding the existence and validity of the certificate, also with the certificate chain up to the root certificate,
- A qualified electronic time-stamp referring to the signature or seal, also with a certificate chain up to the root certificate.

In doing so, it is up to the user where the data is stored. The user may attach it directly to the signature or seal or the data signed or also keep it in a separate database and ensure its availability by means of a unique reference.[12]

4.2.1.2 Method for long term preservation pursuant to § 15 of the Trust Service Act [VDG] and to [ETSI SR 019 510], [ETSI TS 119 511] and [ETSI TS 119 512]

Methods for long term preservation pursuant to § 15 of the Trust Service Act **[VDG, § 15] and [ETSI SR 019 510], [ETSI TS 119 511]** and **[ETSI TS 119 512],** which is needed to ensure integrity and proof of existence at a certain time, also belong to the security measures necessary for long-term verifiability.

NOTICE: *In **[ETSI SR 019 510], [ETSI TS 119 511]** and **[ETSI TS 119 512]** basic methods for preservation services and basic preservation technologies are described pursuant to **[eIDAS]**.*

*The preservation techniques used in BSI-TR 03125 **[TR-ESOR]** are described in detail in*

***[ETSI SR 019 510]** in the clauses 4.7.3 and 5.2 and B3.2 and in*

*[**[ETSI SR 019 512]***

*- in the clauses **A.1.4** and **A.3.1** concerning the preservation object formats ASiC-E/ASiC-ERS pusuant to **[TR-ESOR-F, Kap. 3.3]** and*

*- in the clauses **A.1.5 und A.3.2** concerning the preservation object formats XAIP und LXAIP pusuant to **[TR-ESOR-F, Kap. 3.1 und Kap. 3.2]** and*

*- in **Annex E** concerning the "Versioning of Preservation Object Container" usable e.g. in connection with XAIPs or LXAIPs.*

[9] "Verification information" is the result of a validity verification of a digital signature or of an electronic time-stamp and all associated certificates that indicate the validity of the signature, seal or time-stamp and the certificates at a certain point in time (normally the time the signature was created).

[10] In addition to the information of whether the certificate is available in the directory, the information from a qualified trust service provider also includes information about the status of the certificate **[eIDAS-VO, Artikel 24(4)]**. Pursuant to **[eIDAS-VO, Artikel 24(3)]** , the qualified trust service provider shall mark revocations in the certificate directory with the date and time at least within 24 hours after the received revocation request. The revocation becomes valid after its publication. Because the revocation status is needed to verify a qualified certificate of a qualified signature or seal pursuant to the **[eIDAS-VO, Artikel 32 b]** or.**[eIDAS-VO, Artikel 40],** when a signature or seal is created , this information should be immediately obtained, verified and stored also for this reason.

[11] Online Certificate Status Protocol (OCSP), client server protocol for the online status inquiry of a certificate at a certification service provider, see http://www.ietf.org/rfc/rfc2560.txt.

[12] In case of a retrieval of an XAIP by an ArchiveRetrievalRequest/-Response these data are to be integrated in the CredentialSection of this delivered XAIP

4.2.1.3 Trust Service Act [VDG, § 15]

The following details are valid pursuant to [VDG, § 15]:

Pursuant to **[VDG, § 15]**, data with a qualified digital signature or qualified time-stamp shall be newly re-secured before the security value of the existing signatures or seals or time-stamps will reduce by time, if it is needed in cryptographically signed form for a period of time that is longer than that during which the signature or seal or time-stamp algorithm can be considered to be suitable (technically secure).

Because verification data also includes electronic signatures or seals or time-stamps, it is also subject to the requirement and measures of long term preservation pursuant to **[VDG, § 15]**. It is only by means of its inclusion in these measures pursuant to **[VDG, § 15]** that the intactness and thus the authenticity of a certificate, a validity request or a time-stamp can be verified in the long term.

[VDG, § 15] does not establish any legal duties, though.[13] The purpose of this technical requirement is limited to the description of a suitable procedure for preservation in the long term.

However, the qualified trust service provider shall inform the signatory or creator of a seal or of a time-stamp pursuant to **[VDG, Point 2, § 13(1)]**, that data with a qualified electronic signature or qualified electronic seal or qualified electronic time-stamp shall be re-secured by suitable measures pursuant to **[VDG § 15]** as needed, before the security value of the signatures, seals or timestamps will be reduced by time. Thus, the application of the procedure shall generally be considered an obligation when dealing with cryptographically signed data.

Even if **[VDG, § 15]** thereby merely establishes an obligation, there could be a legal duty to apply **[VDG, § 15]**. However, this legal duty shall then arise from other laws, standards or contractual provisions. There is always a legal duty to apply **[VDG, § 15]** if the recipient is obligated on the basis of laws or contracts to maintain the special probative value of qualified signed or sealed or timestamped electronic documents.

The German **"Law for Implementing the "Regulation (EU) No 910/2014"" [eIDAS-DG, S. 43]** contains under "Justification, B. Special Part, To Part 2 (General requirements for qualified trust services), to § 15 (long term preservation of evidence)" the following descriptions to the method, how and when the long term preservation of qualified cryptographically signed data shall be done. This means: *The long-term protection of qualified signed documents is currently executed by resigning or re-timestamping of the signed documents. These measures have to be carried out before the used algorithms and parameters are not secure any more. The observation of the security suitability as well as the resigning or re-timestamping is not limited to preservation services (pursunt to the eIDAS-regulation). This can also be done by the data owner of the signed documents itself or by an assigned IT- service provider*

The compliance to prior art will be assumed if the solution adheres to the the Protection Profiles as well as the Technical Guidelines of the BSI on the current status. The conformity to European standards has to be respected.

(German: "Die langfristige Sicherung qualifiziert signierter Daten erfolgt derzeit durch Neusignieren oder erneutes Zeitstempeln der signierten Daten, bevor die verwendeten Algorithmen und Parameter ihre Sicherheitseignung verlieren. Die Beobachtung der Sicherheitseignung und die Neusignierung bzw. das erneute Zeitstempeln ist nicht Bewahrungsdiensten vorbehalten, sondern kann auch von den genannten Personen selbst vorgenommen werden.

Die Einhaltung des Standes der Technik wird jedenfalls dann vermutet, wenn die entsprechenden und jeweils aktuellsten, im Bundesanzeiger bekanntgemachten Schutzprofile und Technischen Richtlinien des BSI eingehalten werden. Auf die Konformität mit europäischen Standards ist zu achten.")

A standard was created with **[VDG, § 15]** that outlines the framework for a technical solution that satisfies the requirements for preservation of evidence. The intention of the procedure standardised by

[13] "Damit wird zugleich klargestellt, dass keine Pflicht besteht, jegliche Daten langfristig zu sichern." [eIDAS-DG, zu § 15, S. 43]

lawmakers is to ensure that integrity and authenticity of the originally cryptographically signed documents is secured continuously.

Based on the prevailing legal opinion (in this respect, see **[ARO 07]**, chapter 4.2.1.1), a long-term protection of qualified digitally signed or timestamped data pursuant to **[VDG, § 15]** is not a (renewed) declaration of intent, but rather a security measure for existing declarations of intent.

The goal of the procedure is to make it possible to assess the integrity of a qualified electronic signature or qualified seal or qualified time-stamp even if the mathematical signature or seal or time-stamp verification is no longer suitable for proving the integrity of the signature or seal or timestamp because of the used algorithm's lack of suitability as a security measure. In order to ensure that the authenticity of qualified electronic signatures or qualified seal or qualified time-stamp can be verified in the long term – despite any security problems that may become known later – securing of integrity is needed that "preserves" the signature or seal or time-stamp at a certain point in time at which these problems were not considered relevant yet. This securing of integrity shall be able to prove that the signature or seal or time-stamp and the signed or sealed or timestamped electronic data already existed at this point in time. For that reason, the securing of integrity shall encompass the data and the signature or seal or time-stamp, and the documentation of the time shall be carried out by a trustworthy third party, e.g. by a qualified trust service provider.

Qualified electronic time-stamps pursuant to the **[eIDAS]** may be used exactly for this purpose. Pursuant to **[eIDAS Article 41** and **42]**, a qualified electronic time-stamp is the signed or sealed electronic certification of a qualified trust service provider that certain electronic data was presented to this trust service provider at a certain point in time.

Pursuant to **[eIDAS, Article 41(2)] it** is true: " *2. A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.* "

The new securing, e.g. signature or seal or time-stamp renewal, shall be carried out in a timely manner, i.e. before the expiry of the suitability for securing of the used algorithms and associated parameters. Corresponding overviews of suitable algorithms are published by **[ETSI TS 119 312]** and **[SOG-IS]**.

The new securing shall encompass all available signatures or seals or time-stamps. This is the only way to retain the overall structure of the documents and the associated electronic signatures or seals or time-stamps and information. Because the new securing is merely a security measure, the (re-)securing may include any number of data. However, it shall be possible to prove that a certain document has been included, in other words, that it was cryptographically re-signed (along with the other ones).

From a technical point of view, electronic time-stamps are also electronic signatures or seals that can lose their technical suitability as time goes by. Before this happens, these electronic time-stamps also have to be preserved in that a new electronic time-stamp is obtained.

[VDG, § 15] does not differentiate based on whether the hash algorithm, the signature algorithm, or both lose their suitability. However, the qualified electronic time-stamp only has to refer to both the signed or sealed data and the signature or the seal, if the hash procedure, that was used, threatens to become insecure. If the hash algorithm is still suitable, then the time-stamp newly to be created only has to refer to the signature or seal of the proceeding time-stamp. This is sufficient, because the data still remains attached to the old signature or old seal of the proceeding time-stamp in a reliable way. From the perspective of security technology, it is not necessary to compute a new hash value for the data in order to perform signature or seal or timestamp renewal.

Furthermore, in order to ensure an efficient new re-securing, also from an economical point of view, it is not necessary pursuant to **[VDG, § 15]** to obtain **a separate electronic time-stamp** for each electronic document that has to be re-signed or re-sealed or re-timestamped. Rather, an electronic time-stamp may refer to any number of signed or sealed or timestamped documents.

From the security technology perspective, this can be done easily. The effect of an electronic time-stamp for securing integrity does not depend on how many electronic signatures or seals are preserved at the same time. It was also already detailed in the official statement on § 18 SigV 1997 that "one (comprehensive) new signature" may be furnished "for any number of signed data".

Thus, it is possible to perform the new re-securing on parts of an electronic archive in an automated manner. A signature or seal for electronic data or also for an electronic time-stamp that is created by means of an automatic process without the help of a person is considered to be an automatic electronic signature or automatic electronic seal. In doing so, it is assumed that a person consciously initiates this process, but he neither verifies the data to be signed or sealed in individual cases before electronic signing or electronic sealing nor does he unlock the signature or seal key[14] in individual cases. Furthermore, creating qualified electronic signatures or seals or qualified time-stamps en masse is also allowed.[15] In **[eIDAS, Recital (52)]**, the remote signature is expressively mentioned and therefore also possible.

4.2.2 Sarbanes-Oxley Act (SOX)

The so-called "Sarbanes-Oxley Act" (SOX) has existed in the USA since 2002. The law applies to all companies that are listed on the New York Stock Exchange. SOX serves to improve the transparency and traceability in companies when being audited by the SEC (Securities and Exchange Commission). Companies are obligated to, among other things, maintain an internal control system for the rendering of accounts, assess the effectiveness of the systems, and have the correctness of the annual and quarterly reports certified. The fulfilment of these obligations is summarised under the keyword "compliance".

Section 802 of SOX in particular, pursuant to which fines are threatened in the event that electronic documents that are subject to retention are destroyed, changed or manipulated, has direct effects on the requirements for the long-term storage of electronic documents. The companies are not only obligated by SOX to protect electronic documents that are subject to retention against intentional deletion, change or destruction, but rather shall also be able to provide evidence that there were no changes to or manipulations of these documents.

4.2.3 Naibutousei - SOX in Japanese

On 15 February 2007, the Japanese "Financial Services Agency" published new requirements for companies listed in the Japanese stock exchange.

Naibutousei, the Japanese standard that is also referred to as J-SOX is based on the requirements of the US-American Sarbanes-Oxley Act of 2002 (SOX). For Japanese companies, J-SOX places similar demands on the companies listed pursuant to the guidelines of the US-American Securities and Exchange Commission (SEC).

4.3 Functional requirements for the preservation of evidence of cryptographically signed documents

The measures for preservation of evidence (as described above in chapter 3.3) are integrated into the context of an overall system in which the documents, the supplemental evidence data (signatures, seals, time-stamps, certificates, certificate revocation lists, OCSP responses, signature- or seal- or time-stamp verification information, etc.) and evidence records (Evidence Records) are stored in an archive/ECM/Long-Term Storage system. This record keeping shall be carried out in a form that ensures the completeness, availability, readability and integrity of the data stored for the entire retention time. In addition to numerous other aspects, this implies, in particular, the use of open, standardised, and unambiguously interpretable payload data formats for which long-term negotiability can be considered as given pursuant to current knowledge and the specifications of which are standardised and publicly accessible. Furthermore, no format conversions may occur during the retention period by means of which the existing digital signatures or electronic time-stamps could become worthless.

The upstream IT business applications shall also fulfil their tasks in a suitable manner. For example, they shall ensure that the documents to be cryptographically signed were digitally signed or timestamped by the signatory or creator of the seal or by a suitable (qualified) trust service provider authorised to do

[14] Pursuant to **[eIDAS, Article 3(13) and Article 26]** also called electronic signature creation data or pursuant to **[eIDAS, Article 3(28) und Article 36]** also called electronic seal creation data

[15] For more detail, see **[ARO 07]**, chapter 4.2.1.2.

so with suitable signature or seal or time-stamp procedures and signature or seal creation devices at the correct time and that the document storing and utilisation of the TR-ESOR-Middleware functions occurs at the correct time and in the correct manner.

The aspects mentioned above are not the subject of this Technical Guideline. The following requirements for the preservation of evidence presume that the overall system fulfils these requirements, though.

4.3.1 Proof of integrity and authenticity

The prerequisite for electronically stored information having any or the intended legal effects is that the data and documents stored are maintained in the way that they were originally composed, i.e. without any subsequent changes and the possibility that the issuer of the document can still be determined without any doubt after a long period of time. This means that:

It shall be possible to keep proof of the integrity and authenticity of the documents and data that is required and shall be provided from a legal point of view for a very long time.

Because the fleetingness and lack of physical presence are features of electronic data and documents, proof of integrity in the sense of this Technical Guideline is the (technical) ability to prove that the electronic information has not been changed.

The determination of the authenticity of electronic data and documents in the sense of this Technical Guideline designates the (technical) ability to be able to recognise and assign the issuer of an electronic document even after a very long time.

For preservation of evidence, digital signatures and electronic time-stamps shall be securely and reliably created, verified, renewed and stored in the quality stipulated in the legal regulations.

In order to maintain the evidence suitability of cryptographically signed data and documents for the duration of the period of storage, the following steps shall also be taken:

The verification data needed for digital signature and electronic time-stamp verification at a later point of time should be obtained directly after the creation and/or verification of the signatures, seals or electronic time-stamps and be deposited with the documents and data to be archived in a form that will be negotiable in the long term.

In any case, the validity verification of the digital signatures or electronic time-stamps shall be comprehensive, complete and designed in such a manner that the fulfilment of the requirements for advanced and qualified electronic signatures or seals or time-stamps that are defined in the eIDAS-Regulation **[eIDAS]** and also in the German Trust Service Act **(**Vertrauensdienstegesetz **[VDG])** can be determined from the results of the verification.

Furthermore, it shall refer to entire certificate chains (signature or seal or time-stamp certificates of the issuer, of the trust service provider and of the root-trust service provider ("trust anchor") and all of the verification data and time-stamps and make it recognisable in a verifiable manner that the certificates on which digital signatures or the electronic time-stamps are based or to which the certificates were attached at the time of signing or sealing or time-stamping were valid, not revoked, and that the algorithms and parameters used were a suitable security measure at the time of signing or sealing or time-stamping. It shall be possible to log and display all verification steps and verification results in a manner that is clearly laid out and traceable.[16]

When validating digital signatures, it should generally be possible to discern the time of signing or sealing from a trustworthy time-stamp of the digital signature (see also **[HK 06]**, p. 85). If such a time-stamp is not available and the existence and authenticity of the digital signature at an earlier point in time cannot be proved otherwise, the validation shall be carried out with regard to the current time.

In order to guarantee the verifiability of cryptographically signed documents beyond the legally prescribed retention times, standardised data formats shall be used when creating the signatures or seals

[16] Because the signature itself is merely represented by a digital character strings, verifiable statements and thus those that support evidence about the authenticity and integrity and thus in the end the authenticity of the electronic data are only possible after a complete signature verification by including the data signed, suitable hardware and software for displaying the data, the signature certificates and the validity inquiries and by means of a conclusive interpretation of the signature certification results. The eCard-API-Framework **[eCard-2]** supports the logging and interpretation of the signature verification results by generating a signature verification report in a standardised format.

or time-stamps. In addition to the actual digital signature data formats, this applies also to the formats of certificates, certificate revocation lists and certificate status inquiries as well as time-stamps. In doing so, the compatibility with the standards and recommendations according to the prior art[17] and especially with the European Implementing Act 2015/1506 EU and the ETSI-Standards cited therein and technical guidelines and recommendations of the German Federal Network Agency (BNetzA) and Federal Office for Information Security (BSI) shall be ensured (in this respect, see **[eCard-2]**).

Digital signatures or electronic time-stamps according to the **[eIDAS]** only make it possible to prove the integrity and authenticity of electronic data if the algorithms on which the digital signatures or electronic time-stamps are based are suitable as security measures from a mathematical and technical perspective. However, progress in the development of computers and new methods of cryptoanalysis could make it possible that the algorithms or their parameters lose their suitability as security measures over the course of time.[18] Durable and verifiable preservation of authenticity and integrity of electronic data thus makes the use of additional security measures necessary that make it possible to prove that cryptographically signed data in particular were stored in an unaltered manner for the duration of the retention periods. Therefore, digital signatures or electronic time-stamps shall be secured by suitable preservation mechanisms in a timely manner before the suitability as a security measure of the cryptographic algorithms used and the associated parameters pursuant to the eIDAS-Regulation **[eIDAS]** and **[ETSI SR 019 510], [ETSI TS 119 511]** and **[ETSI TS 119 512]** and the German Trust Service Act **(**Vertrauensdienstegesetz **[VDG])** expires. These preservation mechanisms shall be carried out pursuant to the legal requirements and in a largely automatic and economical manner.

The primary intention of preservation methods is to ensure the verifiability of the integrity and authenticity of the documents that have already been cryptographically signed. Pursuant to the prevailing legal opinion, it is thus sufficient for preservation methods pursuant to to **[eIDAS, Article 41 Section 2]** and **[VDG, § 15]** if cryptographically signed data is furnished with a qualified time-stamp. The new cryptographic signature can include any data and can also be carried out including cryptographic representations (hash value, encrypted data) of the data cryptographically signed provided that the cryptographic representations represent the data cryptographically signed in an unambiguous manner and the algorithms and associated parameters used for the creation of the representation can still be considered to be suitable security measures at the time of the digital signature or the electronic time-stamp renewal.

Only such probative value of cryptographically signed documents can be maintained that existed from the beginning and, in the end, is determined, of course, based on the requirements which the party performing the storage places on fulfilling the purpose of keeping the evidence or has a duty to do so. The quality of the cryptographic signatures used and the signature or seal creation devices used is of central importance for the probative value of cryptographically signed documents. Thus, it follows that: Only those key lengths and algorithms, that are published by ETSI in **[ETSI TS 119 312]** und **[SOG-IS],** and classified as suitable from the perspective of security technology are to be used for the creation of electronic signatures, seals and time-stamps.

(A4.3-1) Qualified electronic signatures or seals shall fulfil the requirements for advanced electronic signatures or seals, be based pursuant to **[eIDAS, Point (a) and (b) of Article 32(1)** or **Article 40]** on a valid qualified certificate at the time they are created and be created pursuant to **[eIDAS, Point (f) of Article 32(1)** or **Article 40]** with a secure qualified electronic signature or seal creation device. Qualified time-stamps shall fulfil the requirements of **[eIDAS, Article 3(34) and Article 42]**.

The technical security of qualified electronic signatures or seals is achieved by the use of suitable components for the creation of qualified signature **[eIDAS, Article 29]** or seal creation devices **[eIDAS, Article 39]**. Pursuant to **[eIDAS, Annex II]**, the components are to be designed in such a manner that they are protected against unauthorised use and that they make it possible to reliably recognise the falsification of signatures or seals and manipulation of cryptographically signed data.

[17] German: Stand der Technik

[18] The algorithms considered to be secure are listed in **[ALGCAT]** and are updated there regularly.

(A4.3-2) The issuance of qualified certificates is reserved **[eIDAS, Annex I** or **III]** to qualified trust service providers, which fulfil at least the security requirements of the **[eIDAS].** Pursuant to **[eIDAS, Article 34(1)]** a qualified preservation trust service for qualified electronic signatures shall be processed by a qualified trust service provider pursuant to **[eIDAS, Article 3(17)].**

For the long-term securing and verifiability of the authenticity and integrity of cryptographically signed data and documents, it thus follows that:

Qualified cryptographic signatures for stored cryptographically signed electronic data and documents should be created and verified according to the eIDAS-Regulation **[eIDAS]** and the German Trust Service Act **[VDG].**

Additionally, the integrity of non-signed or non-sealed or non-time-stamped data may automatically be ensured from the time of transmission into an ECM/Long-Term Storage by means of cryptographic security measures such as electronic archive (entry) hash values or signatures or seals or (qualified) archive (entry) time-stamps.

5. Functions of Middleware for preservation of evidence

The functions of the Middleware that can be requested by the user (the business application) for the preservation of evidence shall obviously be oriented towards the purposes of the archive and based on them. Not all of the functionalities of an archive system have to be mapped, though.

The first section of this chapter thus describes the functions of the archive system that shall be available and usable **from the user's perspective** and shall therefore also be taken into account by the Middleware. The technical requirements for the Middleware, which can be found in chapter 6, are based on this.

The most important organisational aspects that an agency or company has to observe in order to also actually maintain the probative value of the archived documents are discussed in the second section of this chapter. One should remember here that these notices can only provide a rough orientation and are not a comprehensive security concept that include all organisational needs. In this respect, please refer to chapter 8.

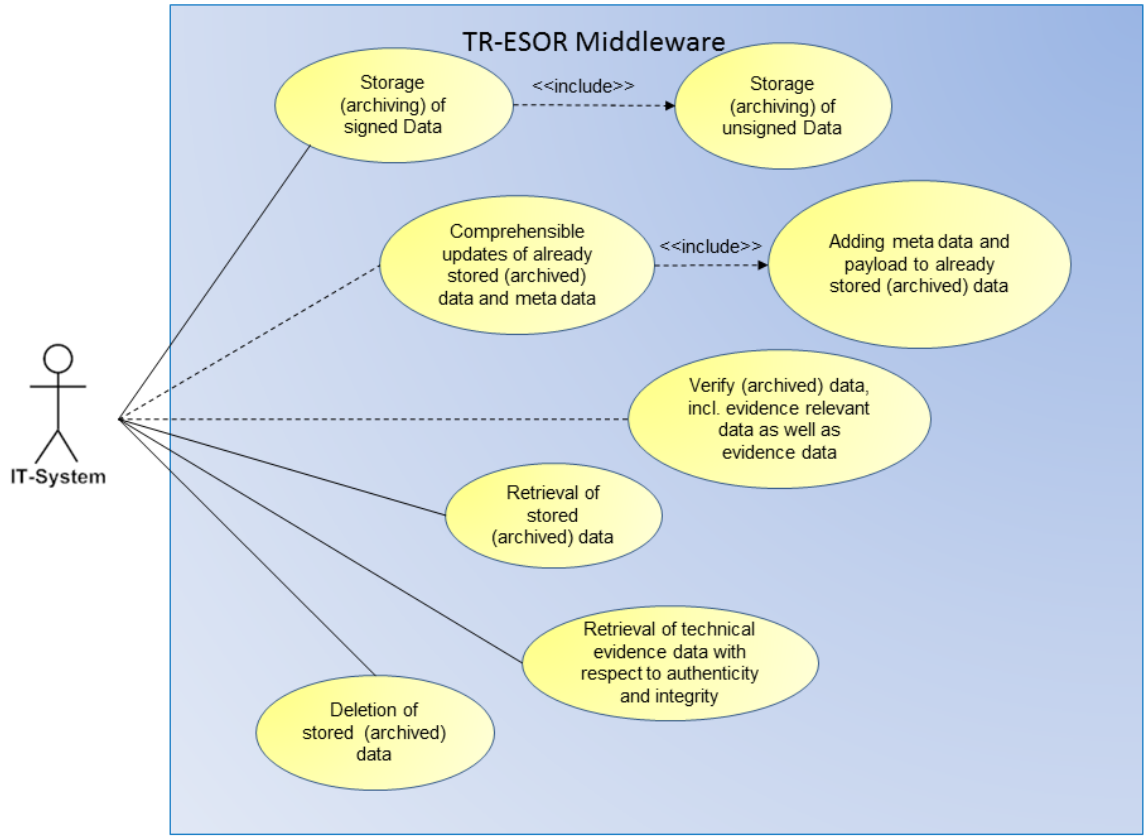


Figure 2: Functional Requirements

The functional requirements determine the minimum functions an archive system and thus the Middleware shall provide for the preservation of evidence from the user's perspective. In doing so, a distinction is made between the following general use cases, as shown in Figure 2:[19]

[19] Additional functions such as "search" (also in a manner that extends beyond business applications) or "structuring in directories" are certainly desirable, but they are not necessary for the preservation of evidence. This Technical Guideline is therefore limited to the obligatory and optional basic functions listed above.

- Storing of (archiving) cryptographically unsigned (that means, not signed and not sealed and not time-stamped) and cryptographically signed data, if applicable, including already available associated supplemental evidence data and Evidence Records,
- Retrieving archived data,
- Updating archived meta data and payload data in a comprehensible manner, which also includes adding additional meta data and payload data to data structures that have already been archived,
- Retrieving evidence records to check the authenticity and integrity of the archived data, and
- Deleting data[20].

It must be noted that even these minimum functions are not necessary in every actual use case. For example, data are rarely changed, but rather only stored, retrieved and, if applicable, deleted in a traditional archive[21]. Therefore, the following functions were defined to be only possible options:

- Targeted retrieval of individual data elements from an individual archive data object (group) without having to return the respective entire archive data object (group) to the IT application.[22]
- Verifying the archival information package including the supplemental evidence data and technical evidence records (Evidence Records) that are contained therein or were additionally transferred.

In general, the following applies:

(A5.1−1) Access to the TR-ESOR-Middleware or the ECM/Long-Term Storage for the purposes of archiving, updating, retrieving data or retrieving technical evidence records or deleting stored documents and data shall always be carried out in a verifiable manner (e.g. logged) by means of defined interfaces from the upstream IT applications. The actions/procedures may only be carried out by persons authorised to do so. Unauthorised access shall be prevented in a reliable manner. The provision of proof shall be carried out in a suitable location of the Middleware, for example in the ArchiSafe-Module.

5.1 Use cases

5.1.1 Archiving cryptographically signed and unsigned data

(A5.1−2) The storage of electronic documents and data (also referred to as "archive data object (groups)" in the following) shall be possible at all times from external IT applications and/or upstream processes through a secure communication channel[23][24].

(A5.1−3) When adding documents and data to the ECM/Long-Term Storage, each archive data object (group) (for an XML-based archive data object (XAIP) pursuant to (**[TR-ESOR-F]**, clause. 3.1) or a logical XAIP (LXAIP) pursuant to (**[TR-ESOR-F]**, clause 3.2, (i.e. a variant

[20] Here, "deleting" means the "irretrievable deletion of data in the agency's long-term storage system". The segregation pursuant to the German Federal Archiving Law (**[BArchG]**) remain unaffected by this. In doing so, the duty to offer to the competent public archive (see also **[TR-ESOR-B]**) applies to agencies pursuant to § 2 Federal Archiving Law or pursuant to the corresponding State Archiving Laws.

[21] This term refers to an archive (system) which is actually only used for the long-term archiving of documents. The so-called "early archiving" and the associated requirement for the changeability of documents is not taken into consideration here.

[22] This function can be used, for example, to create search indices, determine the object owner, determine the minimum retention period, or retrieve electronic signatures.

[23] In this respect, see the information in chapter 8.2.

[24] A secure communication channel is understood to be a transmission route for data that protects the data from being intercepted / read, that at least recognises manipulation or rather prevents it and for which the source and target system are sufficiently strongly authenticated. The strength of the mechanisms used in the respective case depends on the protection requirements of the data transmitted and thus cannot be specified here in a manner that applies to all mechanisms.

of XAIP, where there may be a reference to externally stored data objects in the ECM/Long-Term Storage) or an an ASiC-AIP pursuant to (**[TR-ESOR-F]**, clause 3.3) shall be assigned a unique and, as a rule, unchangeable identifier (archive data object ID, AOID). With the submission of an AOID element during the archiving of cryptographically signed and unsigned data, the AOID may be issued by the application making the request, as for example in the case of a LXAIP.. As a rule, this element is missing and the AOID is provided by the module receiving the request. The AOID makes it possible to find the documents and data stored in a reliable manner and serves as a key for authorised access to the archive data object (groups) stored in the ECM/Long-Term Storage as an archival information package.

In order to prevent the storing of data and documents in a format that is not suitable for permanent and cross-platform storage, the following additional recommendations shall be observed:

(A5.1−4) Prior to storing in the ECM/Long-Term Storage, the Middleware should check the syntax of the archive data object (groups) (for an XAIP pursuant to (**[TR-ESOR-F]**, clause 3.1) or a logical XAIP (LXAIP) pursuant to (**[TR-ESOR-F]**, clause 3.2 or an ASiC-AIP pursuant to (**[TR-ESOR-F]**, clause 3.3) to be transferred for storage for conformity with the data formats defined and specified by the user and operator of the archive system.

a) In the case of non-conformity in case of (L)XAIP or ASiC-AIP, storing in the ECM/Long-Term Storage shall then be denied.

b) In case of an LXAIP, in accordance with a set of rules on base of configurable data, it should be proceeded as follows: The respective error message is stored in the CredentialSection together with all other verification information, if available. After that, the object is stored in the ECM/Long-Term Storage. Additionally, an error message is returned to the IT-application.

(A5.1−5) For the storage of cryptographically signed data, the Middleware shall include the opportunity to verify the digital signatures or time-stamps before they are transferred to the ECM/Long-Term Storage in a comprehensive manner as well on base of the shell model as on base of the chain model or to let them be validated by a (qualified) trust service provider and to deposit the validation results together with the cryptographically signed data. For further processing it is necessary that at least one of both validation models (shell model or chain model) is successful. If both validation models (shell model and chain model) fail, it should be proceeded as follows eventually on base of configurable options:

- a) In case of XAIP or ASiC-AIP: ArchiSafe **[TR-ESOR-M.1]** returns an understandable error message to the application and rejects the archiving of the object.
- b) In case of LXAIP: The appropriate error message is stored in the CredentialSection and, if applicable, together with all further existing validation information. After that, the object is stored in the ECM/Long-Term Storage. In addition, an error message is returned to the IT-application or the XML-Adapter.[25]

NOTICE: *In case of a logical XAIP (LXAIP) the case b), specified above, shall be applied. On base of configurable data the IT-application or the der XML-Adapter may delete the LXAIP and the associated data objects in the ECM/Long-Term Storage after the reception of the error message.*

[25] If at least one signature validation fails, then the return code shall not be any longer "…/resultmajor#ok". If at least chain validation or shell validation does not fail, the return code "…/resultmajor#warning" und "…/resultminor/arl/XAIP_NOK_SIG" should be returned. In all other cases, the return code shall be "../resultmajor#error".

(A5.1−6) For the preservation of evidence of electronic signatures, seals or time-stamps the cryptographically signed data shall be re-protected again by appropriate preservation mechanisms pursuant to the German Trust Service Act **[VDG, § 15], [ETSI SR 019 510], [ETSI TS 119 511]** and **[ETSI TS 119 512]** by including all already existing signatures, seals or time-stamps in the event of the imminent loss of suitability as security measures of the algorithms used for the signature, seal or time-stamp and their associated parameters.

Thus, it follows that:

(A5.1−7) The Middleware shall be able to carry out a legally compliant appropriate preservation measure *"by re-signing or time stamping renewal of the signed data"*[26] (according to **[VDG, § 15]**[27]) of all cryptographically signed data and documents stored in the ECM/Long-Term Storage by means of a request to a qualified trust service provider.[28]

(A5.1−8) The solution for signature or time-stamping renewal (both the procedure and the format of the technical evidence records) shall be compatible with the IETF's "Evidence Record Syntax" standard **[RFC4998]**. Optionally, the XML specification of the Evidence Record Syntax **[RFC6283]** may also be additionally supported (in this respect, see also Annex TR-ESOR-M.3 "ArchiSig-Module" to this Technical Guideline).[29]

(A5.1−9) The permanent proof of the integrity of cryptographically unsigned data and documents may be ensured additionally by an electronic archive entry hash value, and electronic archive entry signature or seal or an electronic archive time stamp at least from the time of the transfer into the archive system. The quality required for the archive entry hash value, the archive entry signature or seal or the archive entry time-stamp is based on the purpose of proof required or intended.[30]

(A5.1−10) The Middleware should provide the possibility that a comprehensive verification report pursuant to **[TR-ESOR-VR]** can be requested for an XML-based archival information package (XAIP) pursuant to (**[TR-ESOR-F],** clause 3.1) or a logical XAIP (LXAIP) pursuant to (**[TR-ESOR-F],** clause 3.2) or an ASiC-AIP pursuant to (**[TR-ESOR-F]**, clause 3.3) including the supplemental evidence data (signatures, seals, time-stamps, certificates, certificate revocation lists, OCSP responses etc.) and technical Evidence Records that are contained therein or were additionally transferred.

5.1.2 Updating data that has already been archived

(A5.1−11) Updating archived documents and data (that preserve evidence) including the associated meta data shall be possible. In the sense of this Technical Guideline, permissible changes to archival information packages are

(1) Adding additional documents, data, meta data, signatures, seals, time-stamps, signature verification information or other evidence records to archival information packages,

(2) Changing meta data,

(3) Logical deleting data or meta data.

---

[26] See "Begründung, B. Besonderer Teil, Zu Teil 2 (Allgemeine Vorschriften für qualifizierte Vertrauensdienste), of § 15 (long-term preservation of evidence (German: Langfristige Beweiserhaltung))"

[27] See also **[ETSI SR 019 510], [ETSI TS 119 511]** and **[ETSI TS 119 512]**

[28] Here, "all [...] in the ECM/Long-Term Storage" means all data and documents that are stored in the ECM/Long-Term Storage and for which preservation of evidence is desired and implemented by using the TR-ESOR-Middleware. The ECM/Long-Term Storage may also hold additional databases for which preservation of evidence is neither needed nor desired.

[29] For merely functional conformity, it is possible to deviate from the strict requirement of compatibility with **[RFC4998]** or **[RFC6283]** if the solution can prove legally compliant signature renewal on the one hand and on the other hand is based on national or international standards.

[30] If unsigned electronic documents are added to the archive, it`s recommended to secure them upon entry of the document into the archive with an initial archive time stamp. This cannot compensate for signing which was not carried out in the past, but it can prove the presence of the document at a certain time. (See **[ARO 07]**, p. 108).

(A5.1−12) U pdates in the sense above may only be made by authorised IT-applications using a secure communication channel to the TR-ESOR Middleware. As a rule, this will be the IT-application that originally archived the data.

(A5.1−13) When updates are made, a supplemental XML-based archival information package (Delta-XAIP- or Delta-LXAIP- element) shall be submitted pursuant to **[TR-ESOR-F]** to which the same requirements for the verification of the data formats and signatures, seals or time-stamps as for archiving apply (see (A5.1-4)0, (A5.1-5), (A5.1-9)).

(A5.1−14) All updates shall be traceable. Thus, all updates shall be made in a new version of the archival information package. Versions of archival information packages that have already been archived shall not be changed anymore. The new version should be created pursuant to **[TR-ESOR-F]**, chapter 3.1.2.[31]

(A5.1−15) The probative value shall not be compromised by updates. This applies to all versions of an updated archival information package. Furthermore, the requirements (A5.1-6) and (A5.1-7) also apply to all versions of an archival information package.

(A5.1−16) The "update" function shall be implemented in such a manner that deleting data, meta data or entire archival information packages is not possible, not even by means of overwriting with empty data structures.[32]

(A5.1−17) All updates should be logged in comprehensible manner. If possible, the time of the change, the author and the contents of the change are to be logged.

5.1.3 Retrieving (returning) archived data

With the retrieval of archived data the archive data object stored in the ECM/Long-Term Storage will be returned.

The retrieval of archived data may concern a self-contained XAIP pursuant to (**[TR-ESOR-F]**, clause 3.1) with complete digital record structures or a logical XAIP (LXAIP) pursuant to (**[TR-ESOR-F]**, clause 3.2) or an ASiC-AIP pursuant to ([**TR-ESOR-F]**, clause 3.3), individual documents or merely certain elements of documents. These differences will not be discussed here, but they will be dealt with again in the technical definitions in chapter 7.

(A5.1−18) The retrieval (return) of archived data shall be carried out from the upstream IT-applications through a secure communication channel.

(A5.1−19) A valid archive data object ID (AOID) shall be transferred to the archive system for the retrieval of archived data.

(A5.1−20) It shall be possible to retrieve each version of an updated archival information package individually and it shall also be possible to retrieve all versions of an archival information package. When retrieving a certain version, it shall be possible to identify the sought version additionally by means of a version identifier, referred to as VersionID in the following.

(A5.1−21) The retrieval of archived data may be supported by additional suitable search functions (in this respect, see also TR-ESOR-M.1, chapter 4.6). These functions, though, do not serve the preservation of evidence and thus do not have to be implemented in the TR-ESOR-Middleware.

(A5.1−22)

[31] Pursuant to **[TR-ESOR-F]**, chapter 3.1.2, the protectedPointers and unprotectedPointers of a versionManifest determine a version in each case.

[32] Overwriting with other contents is the same as changing the contents and shall remain traceable by means of versions. In particular, the original contents of the previous version shall also be maintained in the ECM/Long-Term Storage system.

NOTICE/A5.1-22:

*In case of a logical XAIP (LXAIP) pursuant to (**[TR-ESOR-F]**, clause. 3.2), i.e.. a variant of XAIP, where there may be in the LXAIP a reference to externally stored data objects in the ECM/Long-Term Storage, the retrieval of the archive data object by the IT-application or the XML-Adapter may be done on base of configuration data by two methods*

1) with two steps:

a) Retrieval of the logical XAIP (LXAIP) by requesting it from the TR-ESOR-Middleware

b) Retrieval of the externally stored associated data objects in the ECM/Long-Term Storage from the ECM/Long-Term Storage by requesting it from the Download-Module

or

2) with one step:

a) Retrieval of the XAIP by requesting it from the TR-ESOR-Middleware.

(A5.1–23) The retrieval of archived data may be supplemented by a (configurable) automatic integrity verification of the data retrieved. The custom application would receive proof of the integrity of this data together with the data retrieved. This function, though, does not serve the preservation of evidence and thus does not have to be implemented in the TR-ESOR-Middleware.

(A5.1–24) When retrieving (returning) archived data, it may be requested that the returned (L)XAIP, that means XAIP pursuant to (**[TR-ESOR-F]**, clause 3.1) or logical XAIP (LXAIP) pursuant to (**[TR-ESOR-F]**, clause 3.2) should contain a corresponding Evidence Record in the format specified for each version. This Evidence Record shall be inserted in an `xaip:evidenceRecord-Element` in the CredentialSection and the corresponding version of the (L)XAIP shall be referred to by means of the `VersionID` attribute. If the `versionManifest` is not cryptographically protected itself, an additional `unprotectedObjectPointer`, referring to the Evidence Record in the CredentialSection shall be inserted.

5.1.4 Retrieving technical evidence records

(A5.1–25) The Middleware shall be able to provide technical evidence for the authenticity and integrity of archival information packages. In doing so, the archival information packages are identified based on their AOID.

(A5.1–26) When retrieving proof for the authenticity and integrity of archival information packages, the Middleware shall create and return all technical evidence records[33] needed for this purpose. The technical evidence records shall include all the information that is needed to validate the authenticity and integrity of the data stored, its signatures, seals, time-stamps, certificates and to re-new signature or seal or time-stamp.

(A5.1–27) The Middleware shall be able to create the technical evidence records separately for each version of an archival information package or for all versions of an archival information package together. In the second case, complete proof of the integrity and authenticity since the time of archiving shall be possible even if the archival information package was changed in a controlled manner (versioned) in the meantime.

(A5.1–28) The technical evidence records shall be retrieved through a secure communication channel.

5.1.5 Deleting archived data

At the end of the "life cycle" of an archival information package, i.e. as a rule after the expiry of the legally prescribed periods of retention, the package may be deleted from the archive. Because this is an

[33] "evidence records" here refers to the Evidence Record pursuant to **[RFC4998]** or **[RFC6283]**.

exceptionally critical procedure, execution in a particularly reliable and comprehensible manner shall be guaranteed with suitable technical and organisational measures.

***NOTICE**: After the expiry of the prescribed minimum periods of retention, archival information packages in the public administration may be deleted from the ECM/Long-Term Storage after they have been offered to the competent Federal or State Archive and were assumed by this archive or after the archive issued the authorisation to delete.*

(A5.1–29) The deletion of data and documents **after the expiry** of the legally prescribed periods of retention may be initiated by organisationally authorised users of the technically authorised upstream IT application or by means of a central process that carries out this function for the entire archive and is correspondingly authorised.

(A5.1–30) The deletion of data and documents **before the expiry** of the legally prescribed periods of retention shall be initiated by organisationally authorised users of the technically authorised upstream IT application. The order for deletion shall contain a reason for the deletion.[34]

(A5.1–31) In the case of an order for deletion, all data and meta data as well as all versions of an archival information package shall be deleted in a permanent manner.

(A5.1–32) The conclusiveness of the documents remaining in the ECM/Long-Term Storage shall be preserved in the event of the deletion of other archival information packages.

(A5.1–33) In order to guarantee that the action can be traced, the deletion procedure shall be logged.

(A5.1–34)

NOTICE/A5.1-34:

*In case of a logical XAIP (LXAIP) pursuant to (**[TR-ESOR-F]**, clause 3.2), i.e.. a variant of XAIP, where there may be in the LXAIP a reference to externally stored data objects in the ECM/Long-Term Storage, the deletion of the archive data object shall be done in two steps:*

a) The IT-application or the XML-Adapter Sending sends an ArchiveDeletionRequest to the TR-ESOR-Middleware;

b) The TR-ESOR-Middleware shall delete the logical XAIP (LXAIP) and the externally stored associated data objects in the ECM/Long-Term Storage and then sends back an ArchiveDeletionResponse to the IT-application or the XML-Adapter.

5.1.6 Verifying the archival information package including the supplemental evidence data and technical evidence records that are contained therein or were additionally transferred

(A5.1–35) Through an external interface, the Middleware should provide the possibility to receive XML-based archival information packages (L)XAIP) or ASiC-AIP and to verify them by itself together with the supplemental evidence data (signatures, seals, time-stamps, certificates, certificate revocation lists, OCSP responses etc.) and technical evidence records (Evidence Records) that are contained therein or were additionally transferred or by means of an appropriate validation request to a qualified trust service provider.

(A5.1–36) In this context, the Middleware should also provide the possibility that a comprehensive verification report **[TR-ESOR-VR]** can be requested when an XML-based archival information package (L) XAIP) or ASiC-AIP including the supplemental evidence data (signatures, seals, time-stamps, certificates, certificate revocation lists, OCSP responses etc.) and technical evidence records (Evidence Records), that are contained therein or were additionally transferred, is transferred.

[34] It must be noted here that the corresponding business applications should only implement a function for premature deletion if it is necessary that there is such a function from a technical point of view.

5.2 Organisational requirements

The organisational requirements determine the non-technical requirements that preferably ought to be accomplished before or during the launch of Middleware for the preservation of evidence.

This chapter is intended as a reference for the users of such Middleware and does not define any formal criteria.

5.2.1 Setting up the Middleware for preservation of evidence

The legal representatives of a company or a government agency are responsible for ensuring that a long-term concept for the use of archiving procedures and preservation of evidence is designed in the scope of the IT strategy and coordinated with the IT security concept.

For the preservation of evidence, it shall be guaranteed by the technical or organisational process of archiving that the relevant documents and data for which the preservation of evidence is necessary or has been defined is recorded by the TR-ESOR Middleware.
Furthermore, decisions are to be made about the integration of the TR-ESOR-Middleware into the IT infrastructure, the identification, selection, and management of the data and documents with the requirements for preservation of evidence, and about the regular verification of the conclusiveness achieved.

All logs created by the TR-ESOR-Middleware shall be stored pursuant to the respective relevant legal and/or operational regulations.

(A5.2-1)

NOTICE/A5.2-1): *In case of (L)XAIP or ASiC-AIP there exists the requirement, that the ECM/Long-Term Storage shall archive the associated protocols concerning the storage, the update, the retrieval or the deletion of the archive data objects according to the relevant regulatory laws and provisions and operating rules.*

5.2.2 Requirements for the operational environment

A significant prerequisite for the preservation of evidence is that the legal representatives and employees are adequately aware of the possible risks. To achieve this, the employees involved are to be adequately trained and instructed based on clear and complete procedural documentation.
The description of the process for the preservation of evidence is part of the archiving process and shall be defined in a binding form. The procedural documentation serves to make the processes understandable and thus it is subject to the duty to retain certain documents.

In particular, the following areas with regard to the preservation of evidence are to be regulated in the scope of the process organisation:

- Identification of the documents and data for which the conclusiveness shall be retained,
- Determination of the time of archiving (status of proof),
- Determination of the archive processes including the processes for the preservation of evidence,
- Allowed/desired archive data formats, and
- Definition of the tasks and responsibilities regarding the processes for the preservation of evidence.

The normal operation of the TR-ESOR-Middleware is to be defined in the organisational instructions, i.e. the responsibilities and authorisations of administrators or regulations for change management.

5.2.3 Data protection, data security and confidentiality

All kinds of archiving of electronic information are necessarily subject to general and, if applicable domain-specific regulations and requirements with regard to data protection[35]. Thus, it follows that:

[35] See [2016/679/EU]

The processing for the preservation of evidence of data and documents shall comply with the statutory and domain-specific requirements for data protection and protection of secret information. In particular, the processing and storing of personal data shall be limited to a minimum in the context of digital signatures or electronic time-stamps and the associated validation data. In doing so, it shall also be ensured at the same time that unauthorised persons do not receive access to personal data or other data subject to the protection of secret information under any circumstances.

It shall be possible to fulfil special requirements with respect to protection of data and secret information with a level of effort that is economically reasonable. Thus, it shall also be possible to preserve the conclusiveness of encrypted documents and data.

If digital signatures or electronic time-stamps of the (technical) archivist are needed for certain purposes, e.g. the transformation of data, it should also be possible to use a pseudonym.

6. Derived technical requirements

The following section describes derived and principally technical requirements that are to be fulfilled for the preservation of evidence when a Middleware that complies with this Technical Guideline is set up and operated.

6.1 Technical system requirements

(A6.1-1) In order to avoid solutions that are proprietary, i.e. dependent on a certain product or manufacturer, it shall be possible to guarantee the total logical decoupling of the TR-ESOR Middlware from the IT-Application and the ECM/Long-Term Storage, Furthermore, it shall be possible to guarantee the ability to integrate the middleware into existing information systems and also into those purchased in the future and to guarantee the interoperability, availability, and negotiability of the formats used for payload data, the meta information, the supplemental evidence data (e.g. signatures, seals, time-stamps, certificates, signature- or seal- or time-stamp validation data,, and so on) and technical evidence records (Evidence Records) signatures, time-stamps and signature verification data at least for the duration of the legally prescribed periods of retention.

(A6.1-2) The procedures and technical solutions used for the preservation of evidence of cryptographically signed electronic documents shall not impair the ability to continue to use the electronic documents for various application purposes and in various application systems (custom applications). In particular, no impairments may arise for the procedures and technical solutions used for preservation of evidence, e.g. by signature or seal or time-stamp renewal with respect to:

- The exchange of documents between application systems,
- The change of data formats in application systems,[36]
- The replacement of application systems or components.

(A6.1-3) The TR-ESOR-Middleware should be capable of administering multiple tenants. This means in particular a strict (logical) separation of the archival information packages stored in the ECM/Long-Term Storage, and also a separation of the data relevant to the preservation of evidence (hash trees).

(A6.1-4) The TR-ESOR-Middleware should be able to give the authorized archive access to the chosen mandates (German: jeweiligen Mandanten), in order enable to carry out an assessment during the retention period. The documentation of the decision of the assessment may be done outside of the archive information package.

(A6.1-5) Technical solutions for the Middleware shall support secure external administration and configuration.

6.2 Recommended document formats

This section deals with the formats that may or should be used by the custom applications for the actual payload data – the primary information. In contrast, the next section describes data structures that are recommended for the actual storage in the archive system and which contain payload data as well as meta data and other administrative information.

(A6.2-1) In the interest of long-term availability and negotiability of the documents and data to be archived, only those data formats that make it possible to archive in a manner that is negotiable in the long term in a platform- and manufacturer-independent way should be used.

[36] What is meant here is that the application system can change the data format and that the mechanisms for the preservation of evidence also function with this new data format. More concretely: The functions used for signature renewal shall not be limited to special data formats.
It is assumed in this Technical Guideline that data that has been archived once is not affected by a format change and that a transformation of (signed) data is thus not necessary. If this is the case after all, the results of the TransiDoc project should be referred to; see http://www.transidoc.de.

The organisational concept for electronic administrative work[37] and the Standards and Architectures for E-Government Applications (**[SAGA-5]**)[38], like the Model Requirements for the Management of Electronic Records - **[Moreq10]**[39] promoted by the European Commission, recommend that only a few standardised data formats are used for the long-term storage of electronic written documents.

Chapter 4 of **[TR-ESOR-F]** lists the formats recommended for this Technical Guideline in detail.

6.3 Recommended exchange and storage formats

This section describes data structures that are recommended for the actual storage of payload data (see previous section) as well as meta data and other administrative information in the archive system.

Pursuant to the Program for the Federal, State and Municipal Governments for the Standardisation of Data Exchange with and in the Public Administration[40], the following is recommended for long-term storage and, in particular, for long-term storage with preservation of evidence:

(A6.3-1) Pursuant to the recommendations of national (**[SAGA-5]**[41], **[XÖV]**[42], **[ArchiSafe]**) and international (**[MoReq10]**[43], **[OAIS]**, **[OASIS]**[44]) standardisation initiatives, content data, meta data and validation data[45] for data and documents to be stored in the long term should be stored and managed in a self-contained and self-explanatory archival information package on the basis of XML (abbreviated as **XAIP** for: **X**ML formatted **A**rchival **I**nformation **P**ackage[46]) or a logical XAIP (LXAIP) pursuant to (**[TR-ESOR-F]**, clause 3.2) or an ASiC-AIP pursuant to (**[TR-ESOR-F]**, clause 3.3) and a formalised document type description in XML syntax (XML schema).[47]

(A6.3-2) In addition to the requirement (A6.3-1) page 39, they shall be returned in a self-contained and self-explanatory exchange format on the basis of XML and pursuant to a formalised document description in XML syntax (XML schema) – regardless of the storage format actually used in the ECM/Long-Term Storage – in the case of a request for or export of the data and documents to be stored.

The storage or at least the exchange of data and documents in a self-explanatory archival information package based on XML not only supports the platform and product neutrality but also the ability to migrate archived data while preserving evidence.[48]

---

37 See http://www.verwaltung-innovativ.de/DE/E_Government/orgkonzept_everwaltung/orgkonzept_everwaltung_node.html

38 See http://www.cio.bund.de/Web/DE/Architekturen-und-Standards/SAGA/saga_node.html

39 See http://www.moreq.info/

40 The standardisation of data exchange coordinated on a federal, state and municipal level is intended to make data connections that are automatic and free of media discontinuity possible between municipalities and state and federal agencies and their customers. The goal of this project in the scope of the "Deutschland Online" action plan is to create a joint general concept supported federally, on a state level and locally for the development and nation-wide use of standardised technical data formats and data structures (technical standards) and technical interfaces for the electronic exchange of business and administrative messages within and with the public administration on the basis of XML. For more information, see http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Projekte/Aktionsplan%202009.html

41 See http://www.cio.bund.de/Web/DE/Architekturen-und-Standards/SAGA/saga_node.html and especially http://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/SAGA/saga_modul_tech_spez_de_bund_5_0_download.pdf, chapter 13, p. 74 et seq.

42 See http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Projekte/Aktionsplan_2011.html

43 See http://www.moreq.info/

44 See http://docs.oasis-open.org/

45 This concerns the signatures and associated certificates as well as the verification information for both. In the case of a migration to a new archive system, the ERS evidence records from the old archive system could also be included here.

46 The designation follows the notation of the reference model for Open Archive Information Systems (OAIS) of the National Aeronautics and Space Administration of the USA. For more information, see http://public.ccsds.org/publications/archive/650x0b1.pdf

47 It must be noted that the volume of binary content data is increased by approx. 36% if it is encoded in BASE64 for embedding it in an XML package. Thus, the probability that the packages reach or exceed a size that impairs the ability to process them automatically is also increased, if no LXAIP is used.

48 On the syntax level, XML as a text-based meta markup language not only supports the description, but above all it also supports the automatic display, manipulation and processing of logically structured data and, furthermore, it is characterised by good expandability and a high degree of flexibility. On the semantic level, rules and structure definitions in XML syntax (XML schema) support the mapping of structured content models. XML schemata not only allow a

A detailed description of the syntax and semantics of a suitable XAIP oder LXAIP oder ASiC-AIP-Container can be found in chapter 3 of the Annex **[TR-ESOR-F]** "Formats" to this Technical Guideline.[49]

(A6.3-3) Pursuant to the recommendations of national (**[SAGA-5]**, **[XÖV]**[50], **[ArchiSafe]**) and international (**[MoReq10]**[51], **[OAIS]**, **[OASIS]**) standardisation initiatives, the interfaces for the exchange of data between the components and parts of a middleware that conforms to this Technical Guideline as well as to external components (e.g. the custom applications and the ECM/Long-Term Storage) should generally be described and realised by means of XML and corresponding schema definitions or comparable open, standardised data formats.

In Annex **[TR-ESOR-E]** to this Technical Guideline, the interfaces of the IT Reference Architecture that is introduced below are described in a corresponding manner as an example.

6.4 IT infrastructure

The technical security measures mentioned in the following for the TR-ESOR-Middleware and the entire archive system serve the preservation of evidence and include physical security measures, logical access controls and data backup and outsourcing procedures for normal and emergency operations.

This chapter is considered to be a notice for the users/operators of such a middleware and does not define any formal criteria. More details are to be found in **[IT-GSK-B-A]**, **[IT-GSK-U-A]** respectively **[ETSI TS 119 511]** and **[ETSI TS 119 512].**

The ECM/Long-Term Storage constitutes the data sink of the electronic archive. The archived data and documents are stored here in a secure manner including all of the traffic and administrative information needed for long-term storage and availability.
It may be a storage that includes both the archive data objects and the administrative information and data for securing the integrity and authenticity (the hash trees among other things). Both kinds of data may also be deposited in different storage media.

This may be any kind of storage system (SAN, NAS, hard drive system with any kind of file system, relational database, object-oriented database, XML-capable database, archive system etc.) as long as this system fulfils all other requirements.

The storage system may be divided physically into several storages, even into storages with different interfaces, capacities or physical characteristics, such as media, kind of connection (latency period, bandwidth), locations etc.

For archiving with preservation of evidence, the IT infrastructure and storage media shall be protected against loss, destruction and unauthorised changes by means of physical security measures.
In addition to the mechanisms for access protection in the upstream IT applications, a suitable authorisation concept shall also be implemented in the ECM/Long-Term Storage in order to protect the archived data and documents.

The overall system shall stipulate and implement suitable measures to reliably prevent impermissible manipulation or the impermissible exchange of components or modules of the system.

Backup copies of the storage media may be made and relocated to a place that is physically remote from the archiving system.

In order to secure the readability of the storage media for the entire period of retention, controls and measures depending on the type of media are to be stipulated, such as regular tests of the readability of the storage media.

---

formal and machine-readable description of an XML vocabulary allowed for the exchange of data, but they also allow the development of complex data structures and the formulation of processing instructions.

[49] Annex **[TR-ESOR-F]** to this Technical Guideline describes general syntactic and semantic structures for an archival information package, electronic data formats for the long-term storage of payload data and meta data as well as structures, formats and algorithms for the creation and interpretation of cryptographic data that are suitable for the long-term verification of the integrity and authenticity of electronic documents (packages).

[50] See http://www.deutschland-online.de/Standardisierung.

[51] See http://www.moreq.info/

If the archiving systems (incl. the Middleware) are designed in a redundant way, it shall be tested whether the take-over of function occurs in an orderly manner in the event of a breakdown of a subsystem and whether the data in the systems is recovered in an orderly manner upon the start-up of the system that broke down.

In order to secure the operation of the archiving system (incl. Middleware), the measures to be taken in the event that an archiving system or Middleware fails shall be written down in an emergency plan. In the event of an unplanned interruption, it shall be ensured that the consistency of the data is guaranteed.

This is of particular importance for the data of the TR-ESOR-Middleware. Even a small inconsistency means that the proof of the integrity and authenticity of the archived data and documents can no longer be provided in a reliable manner.

6.5 IT applications using archiving procedures

In addition to the requirements for the IT infrastructure and, of course, the TR-ESOR Middleware, the upstream custom applications shall fulfil various requirements, too.

This chapter is considered to be a recommendation for the users/operators of a TR-ESOR-Middleware and does not define any formal criteria.

As a rule, the IT applications used for archiving are software systems that have to be adapted to the characteristics and archiving requirements that are specific to the organisation. An application in the sense of this Technical Guideline may consist of multiple individual components or programs. It does not necessarily have to be a monolithic program or an individual system. The documents and data to be archived later are created and processed in the upstream application systems. In doing so, they remain on the data storage media associated with these application systems until the time of archiving.
The IT applications or IT services used for archiving should fulfil the following basic requirements:

- The creation of data to be archived in defined standardised data formats that are negotiable in the long term (e.g. PDF/A or XML, see chapter 6.2).
- If required by legal or other regulations from a technical point of view, the application or the user shall be able to provide the payload data to be archived with a digital signature or electronic time-stamp in the quality required by the legal regulations or other regulations before it is stored in the archive system.[52]

  In order to be able to prove the validity of the digital signature or the electronic time-stamp during the term of the legally required retention periods, it is recommended that all validation data needed to prove the validity of the digital signature or electronic time-stamp is obtained during creation of the digital signature or electronic time-stamp and that it is stored together with the digital signature or time-stamp data within the data storage of the business application. The scope of the required validation data is based primarily on the goal of the required securing of proof (in this respect, see also clause 4.1). [53] [54]
- Furthermore, the application shall offer a function to verify digital signatures or electronic time-stamps , even those electronic signatures, seals or time-stamps, that were not created by the application itself (e.g. if the application was replaced by another in the meantime). [55]
- For the display of qualified signed, sealed or time-stamped electronic data and documents, the application or the application environment should make a trustworthy display component (Trusted Viewer) available.

[52] Of course, the cryptographic functions offered by the TR-ESOR-Middleware may be used for this purpose.

[53] Pursuant to **[SFD 06]**, verification data does not necessarily have to be obtained and stored if it is retained by the certification service provider for at least as long as the signed document shall be retained.

[54] The background of this requirement is that there can be a long period of time between the actual archiving and the creation of the signature. While, pursuant to the recommendation, the archive system does verify the signature contained upon archive entry, it can only verify the validity of the certificates used at the time the signature was created if the certification service providers still have such information. If this is not (or no longer) the case, then the signature contained cannot be verified and the probative value of the data is effectively lost.

[55] For the verification of signatures, the application can also use the functions of the TR-ESOR-Middleware.

- The IT applications shall have interface functionalities for the storage of the documents and data to be archived.
- The IT applications shall have interface functionalities for retrieving and deleting[56] documents and data that have already been archived and retrieving evidence records to prove the authenticity and integrity on the basis of the archive data object IDs (AOID) and, if applicable, VersionIDs returned by the archive system or Middleware and shall have interface functions for updating data that has already been archived and verifying the archival information package including the supplemental evidence data or technical evidence records that are contained therein or were additionally transferred.

  In doing so, the deletion process is not initiated by the ECM/Long-Term Storage or the TR-ESOR-Middleware, but by the IT-Application or the XML-Adapter. After the deletion request of the IT-Application or the XML-Adapter the deletion is processed by the TR-ESOR-Middleware together with the ECM/Long-Term Storage. A complete and explicit deletion (in the sense of destruction in a manner that cannot be restored) of archived objects shall be possible even before the expiry of the retention period indicated upon archiving.
- The ability to log archive operations that have been executed.
- The reliable management and assignment of archive data object IDs (AOIDs) to the associated business processes and the place at which the archived data was stored[57].
- The IT applications shall have secure access protection mechanisms on the basis of a reliable and configurable authorisation system. The application or the application environment shall therefore have its own reliable and secure identification and authentication system. It shall be ensured organisationally that only authorised users actually receive or possess the authorisations needed within the application.

[56] In the case of a (federal) agency, the IT application requests the deletion of the document in the long-term storage system after the document has been handed over to the Federal Archiving Agency.

[57] Of course, the migration of the AOIDs shall also be taken into account upon the migration of custom applications. This is the only way that the new custom applications can access the archived data from the old application in the future.

7. IT architecture

The IT architecture of a Middleware for preservation of evidence that conforms to this Technical Guideline shall reliably implement and fulfil the requirements listed in this Technical Guideline (in particular the required functionalities from chapters 5 and 6 and the requirements from chapter 4).

In this section, a (functional) IT Reference Architecture that is independent of a certain manufacturer or product and that fulfils all of the listed requirements is recommended and may therefore be the basis of a corresponding implementation. Based on this IT Reference Architecture, logical system components and interfaces identified on the base of the IT Reference Architecture will be roughly identified and described. The additional detailed specifications of the identified logical components and interfaces take place in the annexes to this Technical Guideline.

NOTICE: *Please note that the distribution of functions to the modules of the IT-Reference Architecture described here is not mandatory. However, a Middleware that conforms to this Technical Guideline shall offer all functions in the required quality with the necessary level of security.*

7.1 Recommended IT Reference Architecture

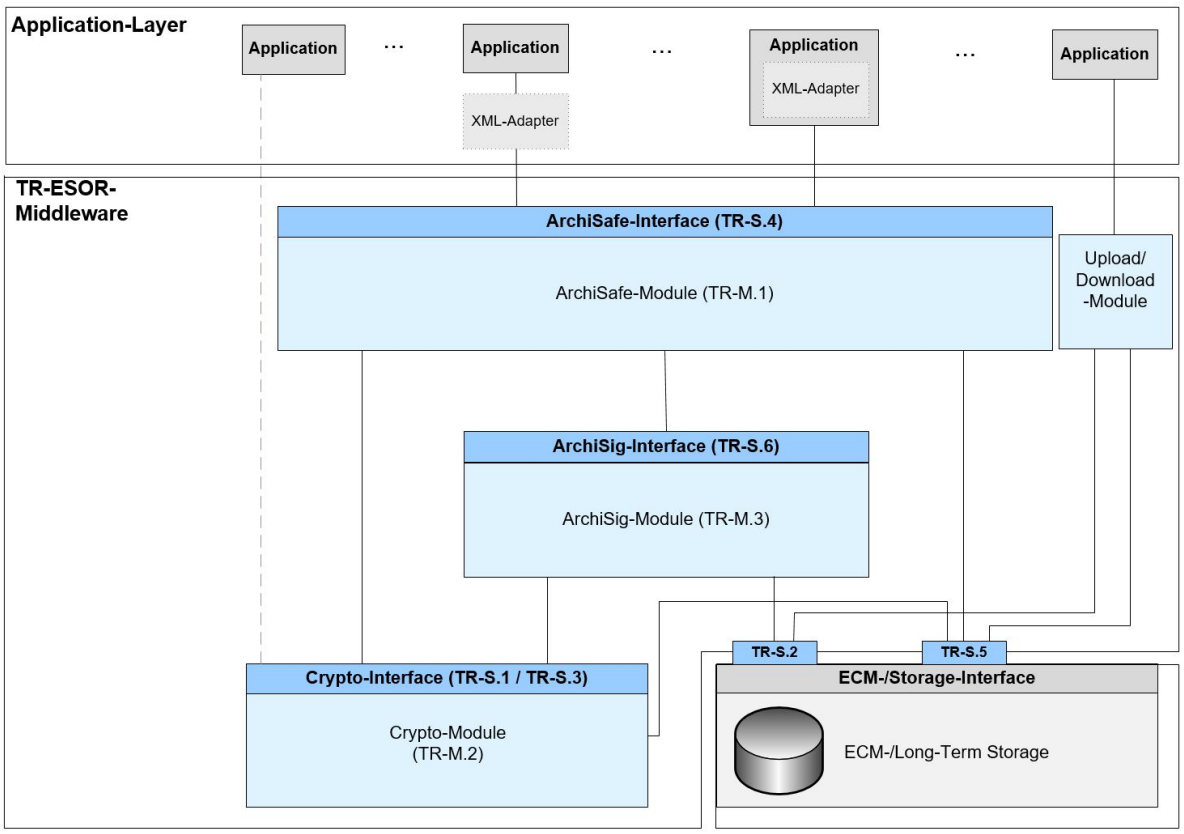


Figure 3: Overview of Reference Architecture

The recommended IT Reference Architecture is depicted in Figure 3 and consists primarily of the following components and interfaces that are roughly described below. They will be described in more detail in the annexes to this Technical Guideline. Furthermore, the graphic shows the external components and systems that complete the picture.

External components and systems

- Upstream applications (for example, an ERP system, a DMS system, an e-mail system, an XML-Adapter or the like) that use the Middleware and thus indirectly the ECM/Long-Term

Storage for the long-term storage of electronic data and documents with preservation of evidence.

- An ECM/Long-Term Storage for the actual data storage. This includes both the storage of the actual archive data objects (groups) and all of the additional data created and managed by the Middleware for securing the conclusiveness. The cryptographic evidence records created by the ArchiSig-Module should at least be stored in a logically separated manner in their own storage area or, preferably, in a physically separated manner in their own storage unit.
- Trust service providers for (qualified) electronic signatures, seals, time-stamps and certification (not depicted) that offer corresponding services to the TR-ESOR-Middleware. These may be separate organisations that offer their services through the internet, but also, for example, privately operated purchased devices that have a corresponding certification and approval.

Modules and interfaces of the TR-ESOR-Middleware

- The ArchiSafe-Module (**[TR-ESOR-M.1]**) that is to ensure a decoupling of the application systems from the ECM/Long-Term Storage and effective and reliable control of access to the ECM/Long-Term Storage.
- A Cryptographic-Module (**[TR-ESOR-M.2]**), that makes all functions available that are necessary for creating hash values, validating electronic signatures or seals or time-stamps, verifying electronic certifications and for obtaining qualified time-stamps or (optional) electronic signatures or seals for the Middleware and that has at least one interface to a (qualified) trust service providers.[58]
- An ArchiSig-Module (**[TR-ESOR-M.3]**) that provides the required functions for signature or seal or time-stamp renewal and creating cryptographic proof (for example, an Evidence Record pursuant to **[RFC 4998]** or **[RFC6283]**[59]) for the integrity of archived data objects (groups).
- The **optional** Upload-Module enables the high-performance upload (storage) of archive data objects, associated to a logical XAIP (LXAIP) pursuant to (**[TR-ESOR-F]**, clause 3.2), in the ECM/Long-Term Storage.
- The **optional** Download-Module enables the high-performance download (retrieval) of archive data objects, associated to a logical XAIP (LXAIP) pursuant to (**[TR-ESOR-F]**, clause 3.2), from the ECM/Long-Term Storage.
- The interfaces between these modules, including among others:
  - The interfaces between the upstream applications and the ArchiSafe-Module. The suggested application-specific XML-Adapter maps the archive interface to an interface that is specific to the application.
  - The interfaces between the internal and external components of the Middleware (named pursuant to the **[TR-ESOR-E]** schema).

The frame referred to as "TR-ESOR Middleware" in Figure 3 shows the scope of this Technical Guideline as regards content. Neither the custom applications nor the ECM/Long-Term Storage nor the trust service provider (not depicted) are subject of this Technical Guideline.

7.2 Requirements of the external interfaces

Based on the requirements listed above, this section makes recommendations and requirements in which manner these requirements should be implemented for the following external interfaces:

a) IT-Application/XML-Adapter – ArchiSafe-Module (TR-S.4) or

[58] This module can also have functions for the encryption and decryption of archived data if this is necessary in the concrete use. Because this is not necessary for the mere preservation of evidence, it is not discussed in more detail in this Technical Guideline.

[59] **[RFC4998]** shall, **[RFC6283]** may additionally be supported.

b) IT-Application/XML-Adapter – Upload-Module or

c) IT-Application/XML-Adapter – Download-Module or

d) Upload-Module – ECM/Long-Term Storage (S.2) or.

e) Download-Module – ECM/Long-Term Storage (S.2) or

f) IT-Application/XML-Adapter.

The same procedure may be used for all other interfaces.

(A7.2–1) In order to be able to process any data format and to be able to link the cryptographic data and meta data with the payload data, the XAIP container defined in (**[TR-ESOR-F],** clause 3.1) or the LXAIP container defined in (**[TR-ESOR-F],** clause 3.2) or the ASiC-AIP container defined in (**[TR-ESOR-F]**, clause 3.3) shall be used as the central data element in the protocol. For the protocol, this means in particular that all data is kept in a single self-contained data element (in case of an XAIP or ASiC-AIP) orare logically connected to each other (in case of an LXAIP). The protocol is not responsible for the logical correctness of this data element after receipt.

(A7.2–2) To protect the integrity and the confidentiality during the transmission and to authenticate the requests and answers (responses), a "trusted channel", such as a TLS tunnel, shall be established with certificate-based authentication on both sides prior to any communication between the client module and server module in case of the interfaces a), b), c), d), e) and f).. Neither requests nor answers (responses) shall be sent through insecure channels. Both the client and the server should ensure this.

(A7.2–3) The "trusted channel" shall ensure the integrity and confidentiality of the data transmitted in it with sufficiently strong cryptographic procedures pursuant to **[TR 02102]**. The TR-ESOR-Middleware and if existing, the Upload-Module or the Download-Module or the ECM/Long-Term Storage shall enforce this and shall not accept any weak procedure during the establishment of the tunnel.

(A7.2–4) The "trusted channel" shall be maintained at least for the duration of a transaction60. Request and answers (responses) to a transaction shall be transmitted through the same "trusted channel".

(A7.2–5) If a "trusted channel" is interrupted during a transaction for any reason, the client shall not expect any answer (response) of any kind from the server, e.g. the ECM/Long-Term Storage. In this case, the client shall establish a new "trusted channel" and determine the receipt of the request, the current status or the end of the transaction to the server by means of STATUS requests.

(A7.2–6) The "trusted channel" should be maintained as long as desired and used for any number of transactions (also parallel).

(A7.2–7) A standardised protocol by means of which the technical confirmation of the receipt of a client request is realised among other things shall be chosen as the transmission protocol within the "trusted channel".

(A7.2–8) Recommendation for the protocol between

a) the IT-Application layer and the XML-Adapter, if existing, or

b) the IT-Application or XML-Adapter and the ArchiSafe- Module (TR-S.4)

is SOAP document/literal encoding[61]. The external interfaces of all TR-ESOR-Middleware-components will be published with WSDL; they may be based on an external XML schema.

The protocol between

[60] Here, the term "transaction" includes the client request to a server and the resulting server response to the client.

[61] Literal encoding uses an XML Schema to validate the SOAP data and offers a significantly better performance than RPC encoding especially for large payload data (in this respect, see also **[FC 07]**, p. 76 et seq. or http://www-128.ibm.com/developerworks/webservices/library/ws-soapenc).

a) the IT-Application or XML-Adapter and the Upload-Module or Download-Module and

b) the Upload-Module or Download-Module and the ECM/Long-Term Storage (TR-S.2)

in order to upload (store) or retrieve archive data objects associated with an LXAIP will not be specified further on for some time except these requirements in this chapter 7.

(A7.2–9) Furthermore, it shall be taken into account that the archive modules may process several (many) transactions – also based on several client applications – at the same time.

(A7.2–10) In case of the interface „b) IT-Application/XML-Adapter – Upload-Modul" the Upload-Module shall send back in the technical **acknowledgement of receipt of the client request**

- either an AOID as a biunique **identifier** of the stored archive data object and a filled <xaip:dataObjectsSection> pursuant to ([TR-ESOR-F], chapter 3.2.1) with a link to the external stored data object and a **corresponding checksum** concerning this data object
- or a filled logical XAIP (LXAIP).

7.3 Alternative architectures

If all of the requirements described in chapters 4 to 6 for the Middleware and the preservation of evidence are also fulfilled by another IT-architecture or an adapted IT-reference architecture, such an IT architecture is also allowed in principle. However, the additional descriptions in the Technical Guideline, in particular the detailed descriptions in the annexes, always refer to the recommended IT-Reference Architecture.

7.4 Components and modules

In this section, the different components and modules of the Middleware from the IT Reference Architecture are described; more detailed descriptions and details can be found in the annexes (in this respect, see also chapter 10 Anlagen).

7.4.1 ArchiSafe-Module[62] (TR-ESOR-M.1)

The ArchiSafe-Module is a standardised and secure gateway that controls the access from business applications to the ECM/Long-Term Storage.

The goal is the realisation of a strict logical separation of the upstream applications systems (the IT custom applications) from the actual ECM/Long-Term Storage systems.

With regard to the preservation of evidence, the ArchiSafe-Module only uses its main function, though, if XML exchange formats and, if necessary, storage formats (see chapter 6.3) pursuant to **[TR-ESOR-F]** are used. Only in this case is the ArchiSafe-Module able to verify whether the syntax of the archive data object (group) transferred by the custom application to the Middleware is correct. Furthermore, this is the only case in which an ArchiSafe-Module that is standardised, i.e. independent of an archive product[63], is also able to verify included electronic signatures, seals or time-stamps or certificates etc. and enter the results into the archive data object (group) by the Cryptographic-Module before the actual archiving. Thus, the recommendations from chapter 6.3 are emphazised here again.

(A7.4-1) Every (writing/changing/deleting) access by the custom applications to the ECM/Long-Term Storage using the archive functions listed in chapter 5 shall be carried out through the ArchiSafe-Module or in case of a logical XAIP (LXAIP) pursuant to (**[TR-ESOR-F]**, clause 3.2) though the Upload-Modul, which is completely decoupled from the IT-Application and the XML-Adapter; other means of access

[62] The name "ArchiSafe" refers to the E-Government Project "ArchiSafe – Legally Viable and Auditable Long-Term Storage of Electronic Documents" from Physikalisch-Technische Bundesanstalt in 2005 that was promoted in the scope of the E-Government Program "BundOnline 2005". The goal of the project was to specify and implement a service-oriented information technology solution for the legally viable and auditable long-term storage of electronic documents (for more information, see: http://www.archisafe.de).

[63] In this case, an ECM system for the actual archiving (saving) is referred to.

to the Middleware or the ECM/Long-Term Storage by the custom applications shall be ruled out by means of suitable technical measures.

However, it is certainly allowed for the ECM/Long-Term Storage itself to offer interfaces, e.g. for storing or changing, that can be used directly by the custom applications – but then not with the focus on the preservation of evidence and in particular not for the changing of (cryptographically signed) documents previously stored using the ArchiSafe-Module; read-only access would be allowed, though. The ECM/Long-Term Storage may also offer more functions than the Middleware. In this case, direct access to the ECM/Long-Term Storage is permitted.[64]

7.4.2 Cryptographic-Module (TR-ESOR-M.2)

The Cryptographic-Module provides various cryptographic functions that are needed for the preservation of evidence.

This includes primarily the cryptographic procedures needed for the calculation of hash values and validation of electronic signatures or seals or time-stamps and verifying electronic certifications and mechanisms for obtaining qualified time-stamps and (optionally) electronic signatures or seals (see also footnote 52 on page 45).

(A7.4-2) The Cryptographic-Module may be implemented in a variety of specifications:

- As a stand-alone hardware module that is addressed by other modules of the Middleware through special hardware interfaces,
- As a mixture of hardware and software; the other modules of the Middleware access the functions of this module solely through the offered software interfaces, or
- All cryptographic functions are implemented completely in the software. The Cryptographic-Module is included as a library or service and used by other software packages of the Middleware.
- Furthermore, the Cryptographic-Module possesses a connection to at least one (qualified) trust service provider pursuant to **[eIDAS, Article 3(19) or Article 3(20)**].

(A7.4-3) The Cryptographic-Module shall fulfil the requirements according to **[eIDAS, Article 32 and 40]** by itself or in connection with a (qualified) trust service provider.

(A7.4-4) ("conditional") In case of LXAIP, the Cryptographic-Module shall be able to retrieve the associated content of the archive data object concerning the link in the `DataObjectSection` from the ECM/Long-Term Storage in order to validate signatures, seals, time-stamps and the result of hash creations, at least in the case, when these objects are not transmitted before.

(A7.4-5) Because the algorithms and parameters for legally compliant electronic signatures or seals or time-stamps allowed for hashing or for the validation of electronic signatures or seals or time-stamps could change pursuant to **[eIDAS, Article 32 and 40]**, it shall be possible for validation to exchange those algorithms and parameters of the Cryptographic-Module that are no longer suitable and endanger security with algorithms and parameters that are suitable for security in a quick and uncomplicated manner.[65]

(A7.4-6) In the event that the interfaces of the Cryptographic-Module or the entire Cryptographic-Module are implemented in the software, they should fulfil the requirements of the BSI Technical Guideline TR-03112 (eCard-API-Framework) in the respective current valid version.

7.4.3 ArchiSig-Module[66] (TR-ESOR-M.3)

The ArchiSig-Module primarily makes functions available for the preservation and renewal of the probativ value of electronic signatures or seals or time-stamps, for the integrity of the archived data

[64] It is pointed out that the ArchiSafe concept stipulates complete logical decoupling of the custom application and ECM/Long-Term Storage.

[65] If the Cryptographic-Module is also able to create qualified electronic signatures, it also shall be possible for this function to exchange the hash and signature algorithms in the corresponding manner.

[66] The name "ArchiSig" refers to the joint project "ArchiSig – Conclusive and Secure Long-Term Archiving of Digitally Signed Documents" that was promoted between 2001 and 2003 by the Federal Ministry of Economics and Labour in the

objects (groups) and for the creation of technical evidence records (Evidence Records) pursuant to RFC4998/RFC6283[67] (more details can be found in Annex TR-ESOR-M.3 to this Technical Guideline). For all cryptographic functions, the ArchiSig-Module accesses and uses the Cryptographic-Module, which has already been introduced. Therefore, the ArchiSig-Module itself does not have to implement any cryptographic functions.

(A7.4-7) The ArchiSig-Module should have a modular character and thus be easy to exchange.

(A7.4-8) The ArchiSig-Module should be able to work parallel in multiple entities, in particular with regard to the case when performing mechanisms for the preservation of evidence of signatures or seals or time-stamps or with regard to hash values renewal for all archival information packages that are present in the ECM/Long-Term Storage is necessary. In this case, however, there still needs to be a controlling object that controls the work of the individual ArchiSig entities.

(A7.4-9) The individual entities should be able to run both on one and on different machines in order to be able to completely use both the bandwidth and the computing power.

(A7.4-10) During the complete preservation of evidence process of signatures or seals or time-stamps or hash value renewal process of all archive data objects (groups) that are present in the ECM/Long-Term Storage, the ArchiSig-Module shall also be able to serve the ongoing requests from regular operations in an acceptable period of time.

7.4.4 Upload-Module

In case of a logical XAIP (LXAIP) pursuant to (**[TR-ESOR-F]**, chapter 3.2), the **optional** Upload-Module makes it possible, that the IT-Application or the XML-Adapter may upload (store) archive data objects, which are associated to an LXAIP, in the external ECM/Long-Term Storage, before the IT-Application or the XML-Adapter submit the associated LXAIP to the TR-ESOR-Middleware.

The Upload-Module has two **external Interfaces**:

a) to the IT-Application or to the XML-Adapter,

b) to the ECM/Long-Term Storage.

(A7.4-11) The external interfaces, used by the Upload-Module, and the used communication protocols shall fulfil the requirements of clause 7.2.

7.4.5 Download-Module

In case of a logical XAIP (LXAIP) pursuant to (**[TR-ESOR-F]**, chapter 3.2), the **optional** Download-Module makes it possible, that the IT-Application or the XML-Adapter may retrieve the externally in the ECM/Long-Term Storage stored data objects, associated to the LXAIP.

The Download-Module has two **external Interfaces**:

a) to the IT-Application or the XML-Adapter,

b) to the ECM/Long-Term Storage.

(A7.4-12) The external interfaces, used by the Download-Module, and the used communication protocols shall fulfil the requirements of clause 7.2.

7.4.6 XML-Adapter for connecting business applications to the Middleware

The **optional** XML-Adapters are data converters specific to the application or specific to the application type that created a standardised (XML-based) data format for storage based on the (proprietary) data and documents of the upstream applications or conversely support the import of the XML data into upstream IT applications. This can also include the conversion of proprietary data formats in open data

scope of the "VERNET - Secure and Reliable Transactions in the Public Communications Networks" program. The goal of the project was to develop a legally compliant, economical, and powerful information technology solution for the conclusive and secure long-term archiving of digitally signed documents (for more information, see http://www.uni-kassel.de/fb07/fileadmin/datas/fb07/5-Institute/IWR/Ro%C3%9Fnagel/projekte_abgeschlossen/projekt_ArchiSig.pdf and https://www.teletrust.de/fileadmin/files/ag8_isis-mtt-langzeitarchiv.pdf)

[67] **[RFC4998]** shall, **[RFC6283]** may additionally be supported.

formats (e.g. PDF/A). The deposition of open data formats as opposed to proprietary ones has the advantage in the long term that it is possible to read them in any case. Otherwise, there is the risk that the stipulated export function (see chapter 7.5.3) shall not be able to carry out a corresponding conversion in the future.

The standardised communication with the ArchiSafe-Module is also conducted with the XML-Adapter. In doing so, the XML-Adapter assumes the role of a standardised connector.

(A7.4-13) In general, such an adapter may be implemented in a variety of specifications:

- As a (fixed) component of the application, i.e. as an archive interface that is integrated into the application,
- As an independent service that transfers data structures and communications logs into the standardised formats of the electronic archive,
- As a (fixed) (multi-client capable) component of the ArchiSafe-Module.

It is to be ensured, though, in particular in the case of the last variation that, for example, blockades in the XML-Adapter on account of faulty applications or improper functioning with regard to security technology on the part of an individual XML-Adapter do not lead to the total malfunction of the entire ArchiSafe-Module. As a rule, this variation (XML-Adapter as a component in the architecture of the ArchiSafe-Module) is thus not recommended.

In the case of the second option (independent service), it is possible to consider the option to guide several similar applications (e.g. several modules of a SAP system or several SAP systems from different clients of an archiving service provider) into the archive using exactly one XML-Adapter. In this case, however, it is particularly important from a security perspective to ensure that cross-application communication through the XML-Adapter is not possible and that it is not possible for one application to access the documents that were archived by another application.

The first option (component of the application) may, in turn, be split into two alternatives:

- Inherent part of the application. This means that the business application directly implements the archive interfaces.
- Module for the business application. This means that the archive interfaces are implemented in their own separate module (in the sense of a library) that is used directly by the business application. Thus, the business application does not have to be adapted itself in order to be able to use the archive.

(A7.4-14) Based on the overall architecture of the archive and its needs, the XML-Adapter should (if it is available and used) be capable of serving multiple clients.

(A7.4-15) The XML-Adapter shall (if it is available and used) be able to use all functions of the ArchiSafe-Module and, if necessary, also all functions of the Upload-Module or the Download-Module to which it is connected correctly and correctly map secure and reliable communication in both directions (IT-Application and ArchiSafe and, if necessary, IT-Application and Upload-Module and IT-Application and Download-Module).

7.4.7 The communication channels and interfaces within the TR-ESOR Middleware

The IT-Reference Architecture includes various interfaces within the Middleware and also the external components (described in more detail in Annex **[TR-ESOR-E]**).

In doing so, a differentiation can be made between

- External interfaces: to the IT-Applications, to the ECM/Long-Term Storage and to the qualified trust service providers
- Internal interfaces: e.g. between the ArchiSafe-Module and the Cryptographic-Module

The necessary administrative interfaces to the individual components are not included in Figure 3. As a rule, they are developed in a product-specified manner (e.g. as a text-based interactive interface, as a

configuration file, as a web-based administration interface etc.) and only play a subordinate role for this Technical Guideline.[68]

(A7.4-16) Interfaces for the administration of the entire Middleware or individual components may only be accessible by persons who are explicitly authorised.

(A7.4-17) Interfaces for the administration of the entire Middleware or individual components shall not compromise the security characteristics of the Middleware or individual components or the integrity and authenticity of the data and documents stored.

7.5 Interaction of the components

The following section illustrates the interaction of the components in the described IT-Reference Architecture in the main use cases (see Figure 3), the storage of electronic data, the updating of archived data, the retrieval of archived data and evidence records, the deletion of archived data and the verification of technical evidence records and supplemental evidence data.

It is assumed in all of the depicted processes that the XAIP or the LXAIP storage format is used. Deviations that arise from the use of another format are not mentioned here.

7.5.1 Storing electronic documents

For the archiving of electronic documents with preservation of evidence, the following basic procedure is stipulated on the basis of the IT Reference Architecture (see Figure 4). In doing so, only the positive case is indicated here in each case for reasons of clarity.

However, all corresponding error inquiries and branches are to be stipulated at all decision nodes. In the event of an error, the process shall be ended with a clear and understandable error message.

Furthermore, it is assumed that each function request and transport of data through an interface mentioned in the IT Reference Architecture is preceded by a successful technical authentication on the network, transport or application layer between the participating modules.

Step 1: **OPTIONAL** - The content data to be archived is provided with a digital signature or electronic time-stamp within the business application or is unsigned. Depending on the data format, the digital signature or the electronic time-stamp may be embedded directly in the payload data or exist as a separate object (e.g. as a file).

Alternatively and also optional – The data that have already been stored in another TR-ESOR system is exported from there together with its supplemental evidence data and technical evidence records with the goal of being stored further in this (new) TR-ESOR system. In this case, you would continue with Step 4.

Step 2: The (cryptographically signed) content data and meta information[69] are then transferred to the XML-Adapter. The format used here depends largely on the business application and thus it cannot be specified in more detail.

Step 3: The XML-Adapter creates an archival information package in XML syntax (XAIP or LXAIP-document) from the (cryptographically signed) content data and meta information pursuant to a defined XML schema (see also chapter 39 and Annex **[TR-ESOR-F]**).

[68] In addition to the functional and technical aspects of the interfaces described in the annexes to this Main Document (data and retrieval formats etc.), aspects with regard to availability and performance are to be observed in particular here. Additional detailed product-specific and project-specific questions with regard to architecture arise from them (e.g. synchronous or asynchronous communication relationships, implementation of data buffers and queues etc.). These cannot be given a general answer, rather they can only be answered with consideration for expected volume of archive inquiries and the size of the individual archival information packages to be stored and the number and locations of the applications to be connected.

[69] Signatures of the payload data that are not embedded directly in the payload data are subsumed here under the term meta data. However, the XML-Adapter treats the signatures somewhat differently and saves them before all of the others in another place in the XAIP – in the CredentialSection.

The format of the payload data and an unique identifier of the corresponding custom application shall at least be entered into the meta data. If the end of the retention period is already known, it should be entered, too. Otherwise, this date should be entered subsequently using the "update" function (see chapter 7.5.2).

Step 4: (“conditional”) Case XAIP: The XML-Adapter transfers the archival information package to the ArchiSafe-Module for archiving through the TR-ESOR-S.4 interface.

Step 5: (“conditional”) Case LXAIP: The XML-Adapter submits (cryptographically signed) content data associated to the LXAIP to the ECM/Long-Term Storage for archiving by an application individual interface and the LXAIP to the ArchiSafe-Module through the TR-ESOR-S.4 interface according to **[TR-ESOR-E]**.

Step 6: The ArchiSafe-Module verifies the access authorisation of the business application on the basis of the identifier transmitted in the request and the syntax of the transferred XML document (L)XAIP on the basis of an XML schema that is stored and authorised in the ArchiSafe-Module. The XML schema is specific to the customer and the application.

Step 7: Supplemental evidence data and evidence records should be transferred to the Cryptographic- Module through the TR-ESOR-S.1 interface for verification.

In the event that the ArchiSafe-Module is configured in such a manner that contained or additionally transferred technical evidence records shall be verified and such technical evidence records are available / were transferred, the ArchiSafe-Module shall transfer the technical evidence records for validation to the Cryptographic-Module through TR-ESOR-S.1 interface.

Step 8: The Cryptographic-Module verifies the mathematical correctness of the digital signatures or electronic signatures.

Notice: *(„conditional“) Case LXAIP:*

If the function call to the Cryptographic-Module includes only a reference as an <asic:DataObjectReference> (see ***[TR-ESOR-F, clause 3.2]****) with a hash value, instead of the necessary archive data object, then the Cryptographic-Module retrieves the associated (cryptographically signed) content data from the ECM/Long-Term Storage by itself.*

Step 9: The Cryptographic-Module validates the validity of the assigned certificates by means of an inquiry at the authorized trust service provider or at the Federal Network Agency pursuant to the GermanTrust Service Act **(**Vertrauensdienstegesetz **[VDG, § 16])**. To do so, a certification path shall be created and verified up to a “root-Trust Service”that is trustworthy from the point of view of the verifying party.

Step 10: The trust service provider provides a confirmation of the validity of the queried certificates as an OCSP or SCVP response (see Annex **[TR-ESOR-M.2]**).

Step 11: The Cryptographic-Module validates the existing technical evidence records and supplemental evidence data up to a root.

Step 12: Depending on the respective case, the Cryptographic-Module returns the results of the validation of the digital signatures and electronic time-stamps and a comprehensive verification report for the verification of evidence records in the form of a `VerificationReport` element (see **[TR-ESOR-VR]**) to the ArchiSafe-Module through the TR-ESOR-S.1 interface.

Step 13: The verification results are entered by the ArchiSafe-Module into the archival information package in the *CredentialSection* of the (L)XAIP document without any changes.

Step 14: The enriched archival information package is transferred to the ArchiSig-Module through the TR-ESOR-S.6 interface for the creation of the initial archive time stamp (see also Annex **[TR-ESOR-M.3]**)

Step 15: The ArchiSig-Module creates a new AOID for this archival information package – if the AOID was not transferred by the application making the request - or has a AOID generated by the ECM/Long-Term Storage and enters this AOID as an attribute into the (L)XAIP document (see Annex **[TR-ESOR-F]**).

Step 16: The ArchiSig-Module enters the canonicalisation algorithm, with which the ArchiSig-Module then canonicalises the (L)XAIP, into the *PackageHeader* of the (L)XAIP.

Step 17: Immediately after that, the ArchiSig-Module has a hash value for the archival information package computed by the Cryptographic-Module through the TR-ESOR-S.3 interface. Details can be found in Annex **[TR-ESOR-M.3]**, chapter 2.4.1.

Step 18: The Cryptographic-Module returns the hash value to the ArchiSig-Module through the TR-ESOR-S.3 interface.

Step 19: The ArchiSig-Module saves this hash value together with the AOID in the hash tree (see Annex **[TR-ESOR-M.3]**).

Step 20: The ArchiSig-Module transfers the archival information package (L)XAIP to the ECM/Long-Term Storage through the TR-ESOR-S.2 interface for persistence.

Step 21: The ECM/Long-Term Storage confirms successful saving, e.g. in case of XAIP by returning the AOID or in case of LXAIP by an returncode.

Step 22: The ArchiSig-Module returns the AOID to the ArchiSafe-Module through the TR-ESOR-S.6 interface as a positive response.

Step 23: The ArchiSafe-Module returns the AOID through the TR-ESOR-S.4 interface as a confirmation of the successful archiving to the XML-Adapter making the request.

Step 24: The XML-Adapter provides the business application with the AOID.

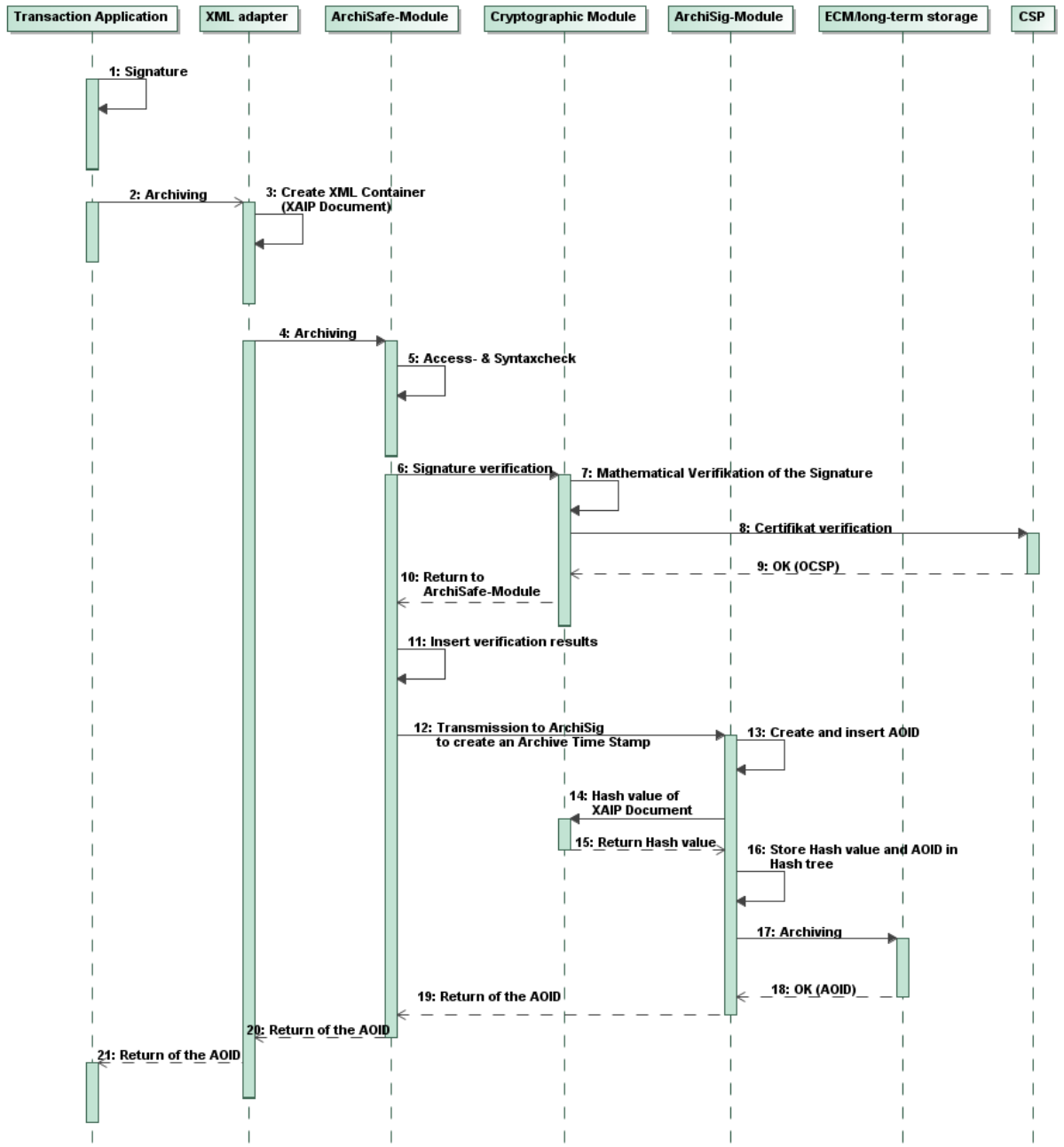


Figure 4: Schematic archiving process in case of XAIP

At a later point in time, the ArchiSig-Module creates an initial archive time stamp for all hash values computed lately and adds it to the hash tree together with the hash values. This process does not have to occur directly during the archiving, but rather, as a rule, it is periodically and automatically initiated. Details can be found in Annex **[TR-ESOR-M.3]**.

7.5.2 Updating archived data

For changing electronic documents that have already been archived with preservation of evidence, the following basic procedure is stipulated on the basis of the IT Reference Architecture (see Figure 5). In doing so, only the positive case is indicated here in each case for reasons of clarity.

However, all corresponding error inquiries and branches are to be stipulated at all decision nodes. In the event of an error, the process shall be ended with a clear and understandable error message.

Furthermore, it is assumed that each function request and transport of data through an interface mentioned in the IT Reference Architecture is preceded by a successful technical authentication on the network, transport or application layer between the participating modules.

Step 1: It is decided on the level of the business application which updates will be made to an archival information package that has already been archived or which additional payload data and/or meta data should be added to an archived information package that has already been archived.

Step 2: **OPTIONAL** - The additional content data to be archived is provided with an electronic signature or an electronic seal or an electronic time-stamp within the business application.

Depending on the data format, the signature or seal or time-stamp may be embedded directly in the payload data or exist as a separate object (e.g. as a file).

Step 3: The content data that is additionally to be archived[70] including the corresponding AOID are then transferred by the business application to the XML-Adapter, if existing. The XML-Adapter generates a supplemental XML-based archival information package (Delta-XAIP- or Delta-LXAIP-element) pursuant to **[TR-ESOR-F]**.

Step 4: The XML-Adapter generates an archival information package in XML syntax from the (cryptographically signed) content data and/or meta information pursuant to a defined XML schema that only contains the updates (delta XML document pursuant to (**[TR-ESOR-F]**, Clause 3.1.6) or Delta-LXAIP-Dokument pursuant to **[TR-ESOR-F]**, clause.3.2.1)). The XML-Adapter transfers the delta XML document to the ArchiSafe-Module for archiving through the TR-ESOR-S.4 interface. In case of a Delta-LXAIP payload data could be submitted additional via an individual interface to the ECM/Long-Term Storage.

Step 5: The ArchiSafe-Module verifies the access authorisation of the business application and the syntax of the transferred XML document on the basis of an XML schema that is stored and authorised in the ArchiSafe-Module.

Step 6: The ArchiSafe-Module should transfer the cryptographically signed data and its electronic signatures or seals or time-stamps to the Cryptographic-Module through the TR-ESOR-S.1 interface for validation.

Step 7: The Cryptographic-Module verifies the mathematical correctness of the digital signatures or electronic time-stamps.

Step 8: The Cryptographic-Module validates the validity of the assigned certificates by means of an inquiry at the issuer of the certificate (usually a Trust Service Provider). To do so, a certification path shall be created and verified up to a trust service provider that is trustworthy from the point of view of the verifying party.

Notice: *(„conditional“) case Delta-LXAIP:*

If the function call to the Cryptographic-Module includes only a reference as an <asic:DataObjectReference> (see ***[TR-ESOR-F, clause 3.2]****) with a hash value, instead of the necessary archive data object, then the Cryptographic-Module retrieves the associated (cryptographically signed) content data from the ECM/Long-Term Storage by itself.*

Step 9: The trust service provider provides a confirmation of the validity of the queried certificates as an OCSP or SCVP response (see Annex **[TR-ESOR-M.2]**).

[70] Signatures of the payload data that are not embedded directly in the payload data are subsumed here under the term meta data. However, the XML-Adapter treats the signatures somewhat differently and saves them before all of the others in another place in the XAIP – in the CredentialSection.

Step 10: The Cryptographic-Module validates the existing technical evidence records and supplemental evidence data up to a root.

Step 11: The Cryptographic-Module then returns the results to the ArchiSafe-Module through the TR-ESOR-S.1 interface.

Step 12: The verification results are entered by the ArchiSafe-Module into the delta archival information package (Delta-XAIP or Delta-LXAIP) in the *CredentialSection* without any changes.

Step 13: The ArchiSafe-Module requests the archival information package that has already been archived through the TR-ESOR-S.5 interface from the ECM/Long-Term Storage. In doing so, the archival information package is identified by the AOID which is not changed by a "update" function.

Step 14: The ECM/Long-Term Storage returns the archival information package to the ArchiSafe-Module. In doing so, the ECM/Long-Term Storage always returns the complete archival information package. This may include several versions.

Step 15: The ArchiSafe-Module adds the updates from the delta archival information package (Delta-XAIP or Delta-LXAIP) to the archival information package requested by the ECM/Long-Term Storage and, in doing so, automatically generates a new version with a new VersionID. Here, it is important that the manifest of the new version lists all data elements that were added, shows the newest version of the corresponding data element in the case of updated data and no longer lists the data elements that are not included in this version anymore (because they were replaced by other/newer data elements). (For more details, see **[TR-ESOR-M.1]** and **[TR-ESOR-F]**.)

Step 16: The complete updated archival information package is transferred to the ArchiSig-Module through the TR-ESOR-S.6 interface for the creation of the archive time stamp (see also Annex **[TR-ESOR-M.3]**)

Step 17: The ArchiSig-Module canonicalises the archival information package with the algorithm indicated in the *PackageHeader* and then transfers it to the Cryptographic-Module through the TR-ESOR-S.3 interface in order to compute corresponding hash values for this archival information package.

Step 18: The Cryptographic-Module returns the calculated hash values to the ArchiSig-Module through the TR-ESOR-S.3 interface.

Step 19: The ArchiSig-Module saves these hash values together with the AOID and the VersionID in the hash tree (see Annex **[TR-ESOR-M.3]**).

Step 20: The ArchiSig-Module transfers the archival information package to the ECM/Long-Term Storage through the TR-ESOR-S.2 interface for persistence.

Step 21: The ECM/Long-Term Storage confirms the successful saving.

Step 22: The ArchiSig-Module returns the VersionID to the ArchiSafe-Module through the TR-ESOR-S.6 interface as a positive response.

Step 23: The ArchiSafe-Module returns the VersionID through the TR-ESOR-S.4 interface as a confirmation of the successful update to the XML-Adapter making the request.

Step 24: The XML-Adapter provides the business application with the VersionID.

At a later point in time, the ArchiSig-Module creates an initial archive time stamp for all hash values created lately and adds it to the hash tree together with the hash values This process does not have to occur directly during the archiving, but rather, as a rule, it is periodically and automatically initiated. Details can be found in Annex **[TR-ESOR-M.3]**.

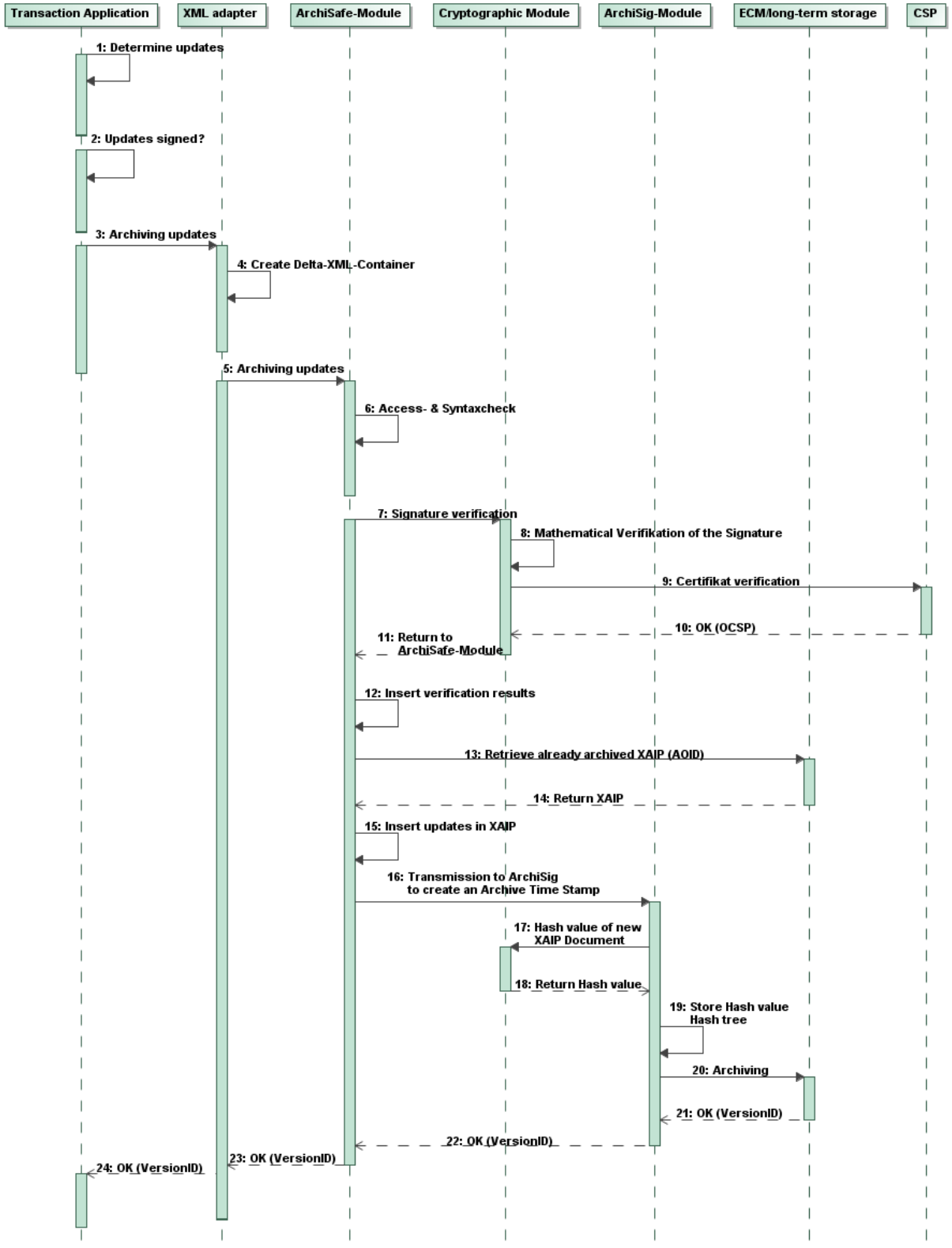


Figure 5: Updating archived data case of XAIP

7.5.3 Retrieving archived data

For retrieving archived electronic documents, the following basic procedure is stipulated based on the IT-Reference Architecture (see Figure 6). In this case, too, the positive case is assumed and the corresponding error checks and branches are not considered in the process for reasons of clarity.

However, all corresponding error inquiries and branches are to be stipulated at all decision nodes. In the event of an error, the process shall be ended with a clear and understandable error message.

Furthermore, it is assumed that each function request and transport of data through an interface mentioned in the IT Reference Architecture is preceded by a successful technical authentication on the network, transport or application layer[71] between the participating modules.

Step 1: The business application makes a request to retrieve archived data to the Middleware through the XML-Adapter. The format of the request is based on the business application.[72] However, the AOID and, if applicable, VersionID or several VersionIDs of the archival information package to be requested shall be included. If no VersionID is indicated, the latest (newest) version is delivered automatically.
In the case of this request, the business application determines with parameters whether the entire archival information package (L)XAIP with or without technical evidence records, only the payload data, only the meta data or a combination thereof should be returned. In the further course, the relevant differences will not be discussed in more detail and the process is described generically.

Step 2: The XML-Adapter sends the request to retrieve archived data to the ArchiSafe-Module through the TR-ESOR-S.4 interface. The request shall contain the archive data object ID (AOID) belonging to the data archived, if applicable the VersionID(s) and a unique identifier of the custom application.

Step 3: The ArchiSafe-Module verifies the access authorisation of the business application.

Step 4: The ArchiSafe-Module requests the archival information package (L)XAIP identified by means of the AOID and, if applicable, the VersionID(s) with or without technical evidence records or the data of an archival information package identified by means of an AOID and, if applicable, VersionID(s) from the ECM/Long-Term Storage through the TR-ESOR-S.5 interface.

Step 5: The ECM/Long-Term Storage returns the archival information package belonging to the AOID and, if applicable, VersionID(s) if applicable including the requested technical evidence records, through the TR-ESOR-S.5 interface to the ArchiSafe-Module. In doing so, the archival information package is reproduced by the ECM/Long-Term Storage exactly to the last bit. Thus, the ArchiSafe-Module receives the archival information package exactly in the same shape in which it was originally archived (see chapter 7.4.1 Step 17 or 7.4.2 Step 20).[73]

Step 6: The ArchiSafe-Module returns the archival information package, if applicable including the requested technical evidence records, to the XML-Adapter through the TR-ESOR-S.4 interface.

Step 7: The XML-Adapter returns the complete archival information package (L)XAIP or the extracted content and meta data to the business application.

---

71 In this respect, see [BLESS 05], page 22, for example.

72 The XML-Adapter does not send an equivalent request to the ArchiSafe-Module in the syntax expected by the ArchiSafe-Module until Step 2. This is why a syntax specific to the business application is still allowed in this step.

73 If the information package was not originally archived in XAIP form, then at this point it still needs transformation into an XAIP. This Technical Guideline does not regulate whether this transformation is carried out by the ECM/Long-Term Storage or the ArchiSafe-Module. It must be noted, though, that the actual payload data (e.g. a PDF file or an e-mail in text format) and signatures shall not be changed during this transformation in order to preserve the probative value of this file.

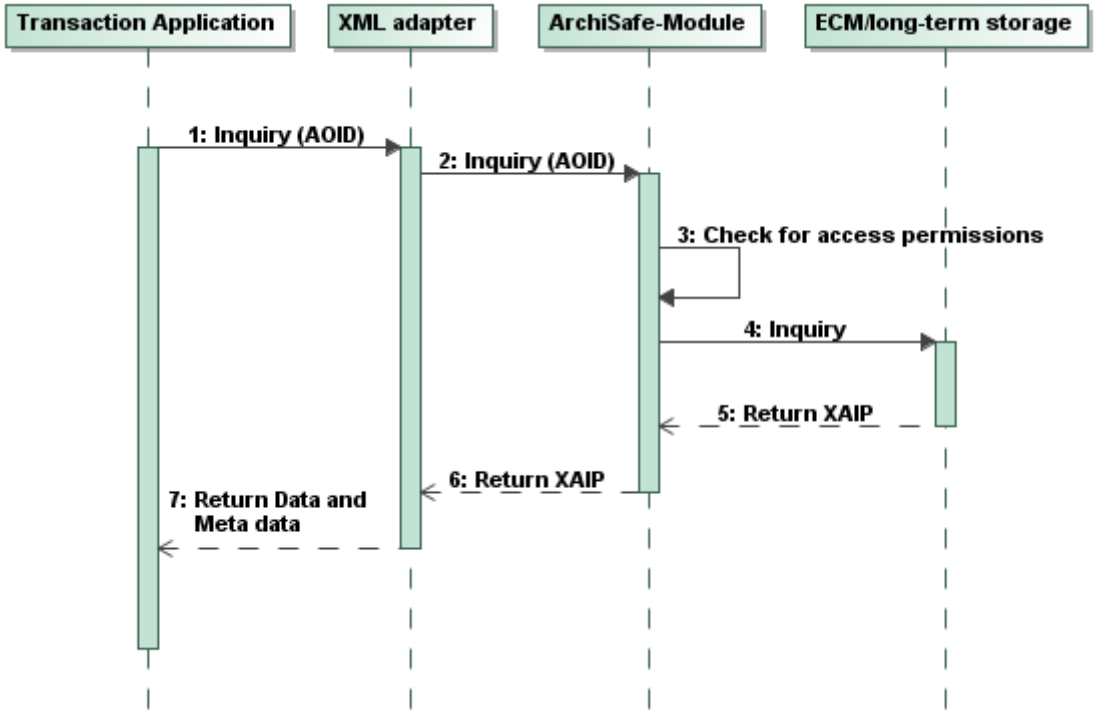


Figure 6: Retrieving archived data in case of XAIP

7.5.4 Returning technical evidence records

To validate the integrity and authenticity of the data archived, the associated technical evidence records can be requested from the Middleware. The process described below is based on the IT Reference Architecture introduced above and only describes the positive case (see also Figure 7). The corresponding error checks and branches are not considered in the process for reasons of clarity.

However, all corresponding error inquiries and branches are to be stipulated at all decision nodes. In the event of an error, the process shall be ended with a clear and understandable error message.

Furthermore, it is assumed that each function request and transport of data through an interface mentioned in the IT Reference Architecture is preceded by a successful technical authentication on the network, transport or application layer[74] between the participating modules.

Step 1: The business application makes a request with regard to the technical evidence records of archived data to the XML-Adapter. The format of the request is based on the business application. However, the AOID and, if applicable, VersionID of the archival information package to be verified shall be included.

Step 2: The XML-Adapter sends the request to retrieve technical evidence records to the ArchiSafe-Module through the TR-ESOR-S.4 interface.

Step 3: The ArchiSafe-Module verifies the access authorisation of the business application.

Step 4: The ArchiSafe-Module makes an inquiry for the technical evidence records of the archival information package identified by means of the AOID and, if applicable, VersionID(s) from the ArchiSig-Module through the TR-ESOR-S.6 interface.

[74] In this respect, see **[BLESS 05]**, page 22, for example.

Step 5: The ArchiSig-Module determines the evidence records in ERS format from the hash tree in its data storage[75] for the archival information package identified by means of the AOID.

Step 6: If there are several versions for this archival information package in the ECM/Long-Term Storage, the Evidence Records shall be calculated for all versions and attached to the result in order to be able to prove the integrity and authenticity of the data since the time of the first archiving if `all` is indicated in the `VersionID` element.
If one VersionID or several VersionIDs was/were specified in addition to an AOID, the ArchiSig-Module shall return the Evidence Record for this VersionID or these VersionIDs. If the `VersionID` element is not indicated, the set of evidence records for the current version of the (L)XAIP is returned.
If the ArchiSig-Module manages several redundant hash trees[76], the corresponding reduced Evidence Record(s) are calculated from each hash tree and embedded in the return value.

Step 7: The ArchiSig-Module returns the calculated Evidence Record(s) to the ArchiSafe-Module through the TR-ESOR-S.6 interface.

Step 8: The ArchiSafe-Module transfers the technical evidence records received to the XML-Adapter through the TR-ESOR-S.4 interface.

Step 9: The XML-Adapter returns all determined technical evidence records to the business application.

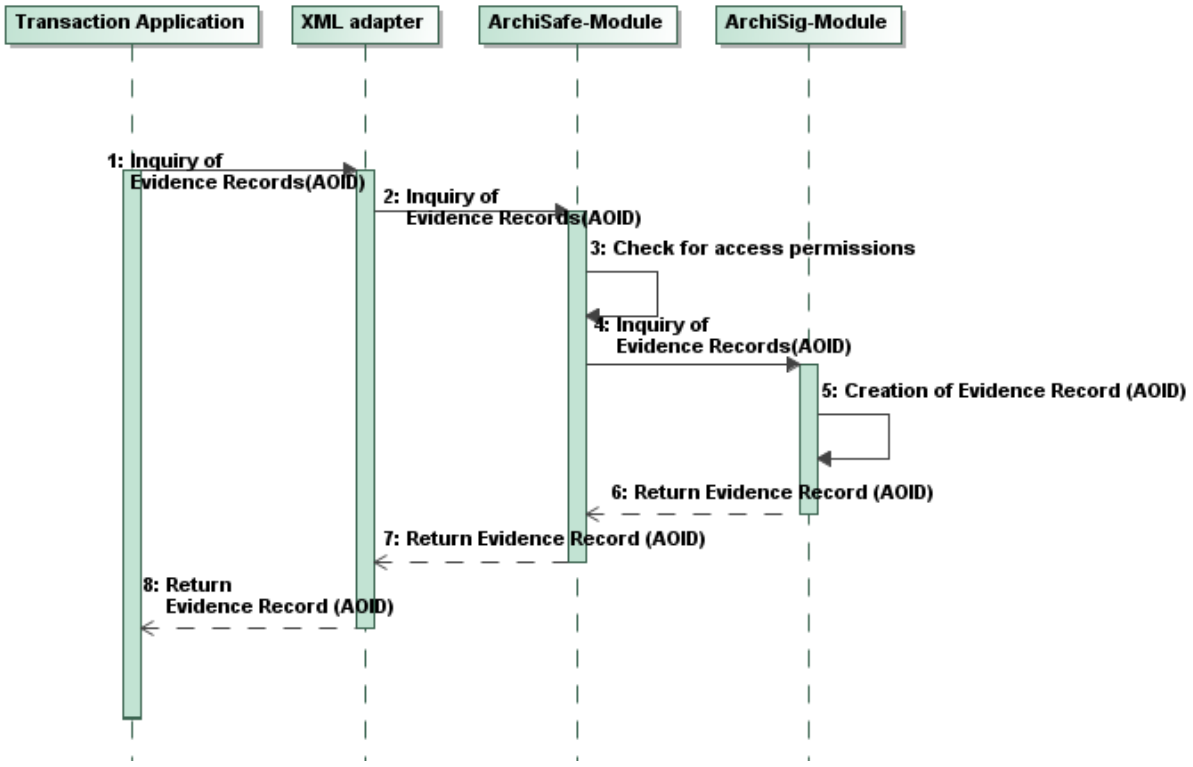


Figure 7: Schematic process of retrieving evidence records in case of XAIP

[75] Pursuant to the IT Reference Architecture recommended in chapter 7.1, the ArchiSig-Module manages its data in a separate storage that is at least logically separated from the actual archive data. The TR-ESOR-S.2 interface does not formulate the corresponding access functions and therefore no reference is made to this interface or the ECM/Long-Term Storage.

[76] See **[TR-ESOR-M.3]** and also **[RFC4998]** or **[RFC6283].**

7.5.5 Deleting archived data

Of course, it shall generally be possible to delete data in an archive. In this respect, however, a distinction shall be made whether the data should be deleted before or after its minimum retention period defined. Premature deletion can become necessary, for example, if personal data has been stored and the person concerned no longer agrees to the storage or objects to it. In any case, the deletion of archived data from upstream IT applications shall only be allowed for persons who are explicitly authorised to do so. The corresponding security characteristics shall be implemented by upstream IT applications. For government agencies, the duty to offer to the appropriate archiving authority shall be observed prior to any deletion (see chapter 5.1.5).

The prerequisite for this function is, of course, that the ECM/Long-Term Storage used or its media allow deletion at all. If this is not the case, the ECM/Long-Term Storage or Middleware is to confirm the request of this "delete" function with an error.

The process described below (see also Figure 8) is based on the IT-Reference Architecture introduced in chapter 7.1 and only describes the positive case. The corresponding error checks and branches are not considered in the process for reasons of clarity.

However, all corresponding error inquiries and branches are to be stipulated at all decision nodes. In the event of an error, the process shall be ended with a clear and understandable error message.

Furthermore, it is assumed that each function request and transport of data through an interface mentioned in the IT Reference Architecture is preceded by a successful technical authentication on the network, transport or application layer of the TCP/IP layer model[77] between the participating modules.

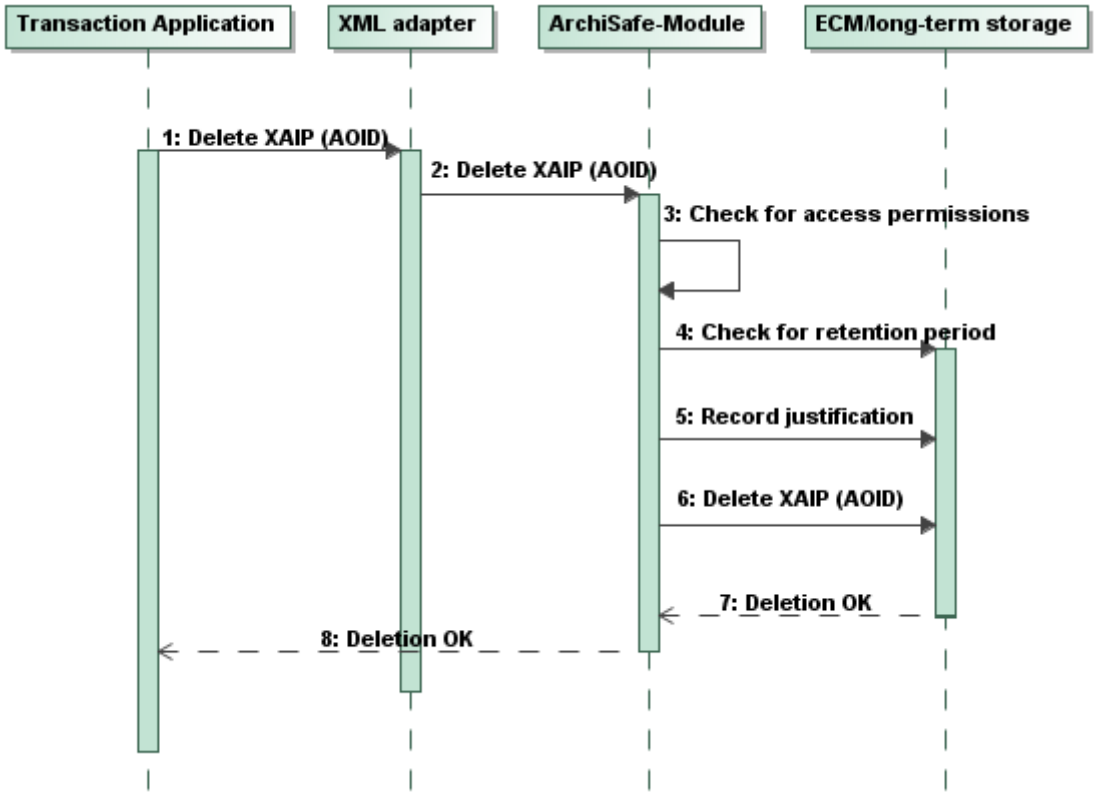


Figure 8: Schematic process of deleting archival information packages in case of XAIP

Step 1: The business application makes a request to delete archived data to the XML-Adapter. The format of the request is based on the business application. However, the AOID of the archival information package to be deleted shall be included.

[77] In this respect, see **[BLESS 05]**, page 22, for example.

If this concerns a deletion before the expiry of the minimum period of retention, the request shall also include a reason for the premature deletion, which will be logged.

Step 2: The XML-Adapter sends a request to delete archived data to the ArchiSafe-Module (through theTR-ESOR-S.4 interface). The request shall include the AOID of the archival information package to be deleted. If this concerns a deletion before the expiry of the minimum period of retention, the request shall also include a reason for the premature deletion, which will be logged.

Step 3: The ArchiSafe-Module verifies the access authorisation of the business application.

Step 4: The ArchiSafe-Module verifies whether the minimum period of retention has already been reached. To do so, the ArchiSafe-Module requests the corresponding meta data from the (L)XAIP from the ECM/Long-Term Storage through the TR-ESOR-S.5 interface.[78] In the event that the minimum period of retention has not expired yet, the ArchiSafe-Module verifies whether the order for deletion includes a reason for the premature deletion.

Step 5: In the event of premature deletion, the ArchiSafe-Module logs the provided reason along with the AOID.[79]

Step 6: The ArchiSafe-Module requests the ECM/Long-Term Storage through the TR-ESOR-S.5 interface to delete the archival information package identified by means of the AOID.

Step 7: The ECM/Long-Term Storage deletes the archival information package[80]. The ECM/Long-Term Storage confirms the success of the deletion operation to the ArchiSafe-Module through the TR-ESOR-S.5 interface. In case of LXAIP two steps are necessary: Deletion of the payload data and deletion of the LXAIP.

Step 8: Because all versions of an archival information package are technically contained within this archival information package, all versions of an archival information package are deleted automatically upon deletion. This is an intended behaviour!

Step 9: The ArchiSafe-Module confirms the successful deletion through the XML-Adapter to the custom application that initiated the deletion operation.[81]

7.5.6 Verifying supplemental evidence data and technical evidence records

The TR-ESOR Middleware should offer the possibility to verify archival information packages including the supplemental evidence data (signatures, seals, time-stamps, certificates, certificate revocation lists, OCSP responses etc.) and Evidence Records pursuant to RFC4998) that are contained therein or were additionally transferred. The process described below is stipulated for this purpose (see also Figure 9).

Step 1: Transferring the XML document to the ArchiSafe-Module

Step 2: The ArchiSafe-Module verifies the access authorisation of the business application on the basis of the identifier transmitted in the request and the syntax of the transferred XML document based on an XML schema deposited and authorised in the ArchiSafe-Module. The XML schema is specific to the customer and the application.

[78] In the event that there are several versions of the archival information package, the minimum retention period for the latest (newest) version is decisive.

[79] This step should always be carried out before the actual deletion so that it can be ensured that the reason is always available even if the ECM/Long-Term Storage breaks down during the actual deletion.

[80] In doing so, it shall be ensured that the data to be deleted is deleted in the ECM/Long-Term Storage in a permanent manner, i.e. made irreversibly unrecognisable on the storage medium.

[81] If the ArchiSig-Module is also to obtain knowledge of a deleted archival information package, this can be initiated by the ArchiSafe-Module at this point.

Step 3: The ArchiSafe-Module transfers the data cryptographically signed and its electronic signatures or seals or time-stamps as well as, if applicable, associated technical evidence records to the Cryptographic-Module through the TR-ESOR-S.1 interface for validation .

Step 4: The Cryptographic-Module validates the mathematical correctness of the transferred technical evidence records and the supplemental evidence data by itself or by a request to a trust service provider.

Step 5: The Cryptographic-Module validates the validity of the assigned certificates by means of an inquiry at the issuer of the certificate (e.g. OCSP request). To do so, a certification path shall be created and verified up to a certification entity that is trustworthy from the point of view of the verifying party.

Step 6: The trust service provider provides a confirmation of the validity of the queried certificates, for example as an OCSP or SCVP response (see Annex **[TR-ESOR-M.2]**).

Step 7: The Cryptographic-Module returns the results of the validation of the transferred technical evidence records and the supplemental evidence data and, if applicable, a comprehensive verification report in the form of a VerificationReport element for the archival information package and/or technical evidence records (see **[TR-ESOR-VR]**) to the ArchiSafe-Module through the TR-ESOR-S.1 interface.

Step 8: The verification results are entered by the ArchiSafe-Module into the archival information package in the *CredentialSection* of the (L)XAIP document without any changes.

Step 9: The ArchiSafe-Module returns the return codes through the TR-ESOR-S.4 interface as a confirmation of the successful verification to the business application making the request.

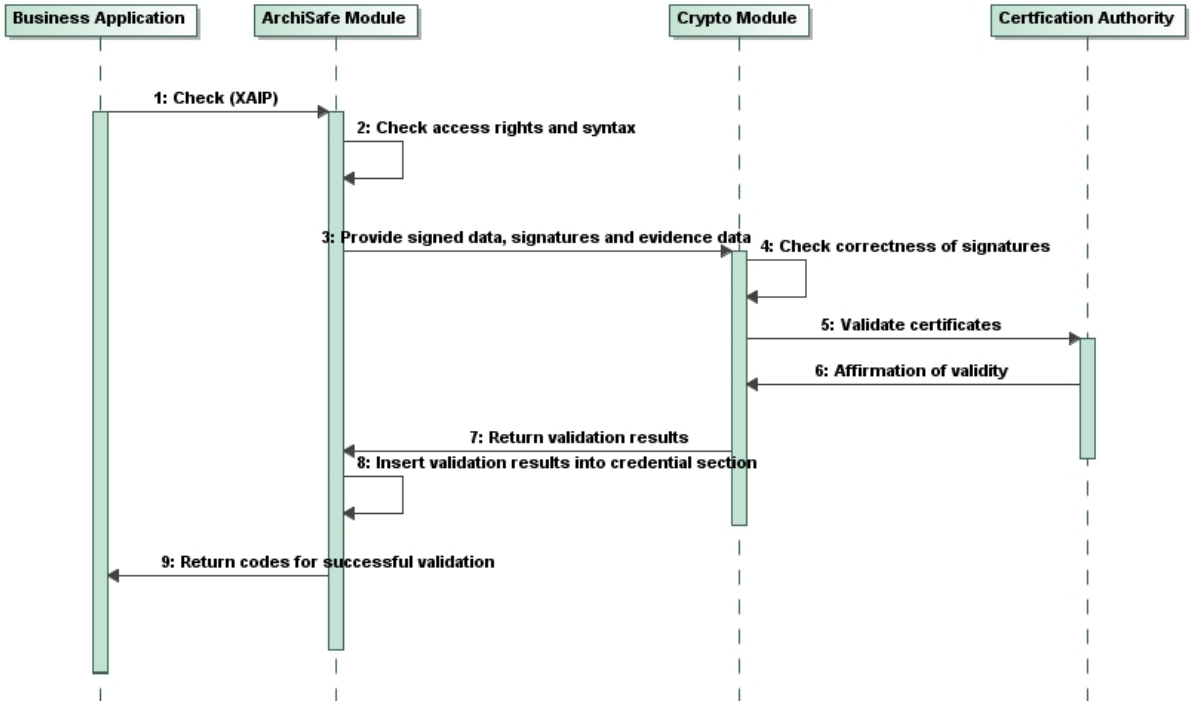


Figure 9: Verifying signatures and evidence records

8. IT security concept

In this section, a generic security concept with regard to the overall system will be developed on the basis of the general requirements in chapter 4 and the IT Reference Architecture recommended in chapter 7.

In addition to the requirements of the Middleware for the preservation of evidence of cryptographically signed data, the requirements of the environment of use to which the custom applications and the ECM/Long-Term Storage belong are absolutely imperative. However, no component of the environment of use is subject of a conformity evaluation based on this Technical Guideline; the characteristics indicated here are only assumed to be a given fact and are merely of informal nature.

8.1 Security objectives

The prerequisite for the storage of documents subject to the duty of retention with preservation of evidence is sufficiently secure archiving procedures. The organisational and technical measures and precautions necessary for this are a component of a security concept that is specific to an organisation and that shall be developed and implemented to guarantee the required level of information security. The components of such a security concept are, in particular, measures and precautions for guaranteeing the following security objectives:

- **Confidentiality**

  The confidentiality criterion requires that the data cannot be viewed, forwarded or published in an unauthorised manner. This requirement is also to be taken into account when an archiving system is being used, in that the Middleware components, actual ECM/Long-Term Storage system, the storage media, any backups, and the communication connections shall be protected against being revealed in an unauthorised manner by means of physical and/or logical access controls.

- **Integrity**

  An electronic archiving system is of integrity if it can be proved that the documents and data to be archived have been stored in a complete and unadulterated manner. In order to guarantee integrity, the ECM/Long-Term Storage as a whole and the documents and data stored shall be protected against manipulation and undesired or incorrect changes. It shall always be possible to detect manipulations and undesired or incorrect changes.

- **Availability**

  The security objective of availability indicates that it shall be possible to select the data and documents intended for storage when required (at all times) within a reasonable period of time in a complete and unadulterated manner from the ECM/Long-Term Storage. This also applies to the validation data created and stored for the purpose of proofing authenticity and integrity.

Additional security objectives for the preservation of evidence can be derived from these basic IT security objectives:

- **Authenticity**

  For the preservation of evidence of archived documents or data, the verifiable authenticity of the documents and data is of decisive importance along with the integrity. It shall be and remain provable without any doubt that a certain (natural) person created or took notice of a certain piece of data at a certain time with the available contents and in the available form. In the case of a long-term archive, this proof shall be possible even after many decades. The authenticity of archived documents and data also includes that the information stored in the electronic ECM/Long-Term Storage is complete (see integrity) and can be assigned without any doubt to a certain business transaction. This security objective is based on the security objective integrity, but imposes significantly higher requirements.

- **Reliability**

  Reliability is understood to be the characteristic of guaranteeing desired legal consequences permanently.

  In general, electronic data are suitable for providing evidence for the desired legal consequences in business transactions. In doing so, the probative value of electronic data largely depends on how one succeeds in proving that the documents have not be changed since their creation or storage (integrity) and that they originate as regards their form and content from the designated issuer (authenticity).

  Furthermore, for the preservation of evidence, binding character means that any operation on the archival information packages during the storage can be documented in a traceable manner. This relates in particular to the revision of meta information and the premature deletion of archival information packages.

8.2 Measures

In order to reach the security objectives indicated above for the Middleware and the ECM/Long-Term Storage in the design of the Reference Architecture, the following measures are required.

This chapter is considered a reference for the users of such Middleware or ECM/Long-Term Storage and does not define any formal criteria.

NOTICE: *It must be noted that this generic catalogue of measures cannot in any case replace a concrete security concept such as one pursuant to the BSI IT-Grundschutz Kompendium 2019 of BSI (see B component OPS 1.2.2 Archiving* ***[IT-GSK-B-A]*** *and Implementation Instructions OPS 1.2.2 Archiving* ***[IT-GSK-U-A]****) that has been adapted to the local needs and circumstances specific to the particular organisation.*

8.2.1 General measures

Before an electronic archive system with a focus on the preservation of evidence is set up, an IT security concept based on a standardised method (e.g. as a concept of an information security management system (ISMS) on base of BSI Standard 200-1, -2, 3. shall be created and implemented with the launch of the system that covers the technical system and all of the relevant processes.

The IT security concept shall be updated regularly (e.g. at least annually).

The measures arising from the IT security concept and its revision shall be implemented quickly to the extent that this is economically reasonable. This applies in particular to the definition and implementation of the responsibilities and competencies, the technical processes as well as the secure administration and control processes.

The set up and operation of an archive system with a Middleware for the preservation of evidence in the sense of this Technical Guideline should be subject to an IT-Grundschutz audit with the goal of certification, in particular for the institutions, organisations, and companies in the public administration in order to be sure that the respective processes and organisations in the archive system's environment of use have been verifiably defined in a purposeful manner.

8.2.2 Measures for the protection of confidentiality

The ECM/Long-Term Storage system and its media shall be operated in rooms with controlled access. Access to these rooms is to be granted only in a very restrictive manner. This also applies to any available redundant systems and backup systems and their media.

The handling and management (transport, storage, disposal) of removable storage media (and backup media in particular in this case) shall be defined in a precise manner and handled very restrictively. Using the backup media shall not simplify access and only expand the group of those able to access (not the same as those authorised to access) to the extent that is absolutely necessary.

The entry of persons into these rooms should be logged and audited on the basis of random samples. Optionally, independent surveillance of the rooms may also be carried out, for example, by means of the use of video cameras.

All actions related to backup media (storing externally, putting into storage, regrouping, verifying the readability, disposal etc.) should be logged. The logs should at least show which person has carried out which action with which media for which reason.

All archive data in the ECM/Long-Term Storage may be encrypted. In such a case, however, special attention is to be paid to secure key management and the restorability of all data in the event of an error. Thus, it is recommended for economical reasons that, if needed, the required processes for encryption and decryption and the connected administration infrastructure are outsourced to external, upstream IT applications. Encryption does not replace the access control mechanisms that are generally needed, though.

The ECM/Long-Term Storage may use backup systems that encrypt the data during the storage on the backup media for the restoration of lost or damaged data. In this case, too, special attention is to be paid to the restorability of data.

If communication connections between individual components of the overall system are not protected by means of other measures (see chapter 49), the physical communication connections shall be kept in secured rooms and/or in secured conduits. It shall be possible to recognise unauthorised access to the lines very quickly.

All communication between the components of the Middleware and with external components[82] may only take place after these components have been successfully authenticated. Here, different levels of authentication shall be considered:

- The authentication procedures shall be designed in such a way that no component of the Middleware or the ECM/Long-Term Storage or the XML-Adapter or Upload-Module or Download-Module, if existing, can be exchanged or bypassed without being noticed.
- The authentication procedures shall be sufficiently strong. In this respect, particular attention shall be paid to whether the communication relationships and components are physically protected or not.
- The authentication of the external service providers used by the Middleware (e.g. the trust service provider) can only be used to the extent the service providers offer this. The opportunities offered shall be used.
- The authentication of external service providers that want to access the Middleware and its components (e.g. for remote maintenance), or which will be accessed by the middleware, shall have sufficient strength so that these systems cannot obtain unauthorised system and data access to the Middleware or to the ECM/Long-Term Storage and its data.
- The authentication of external systems (in this case the business applications in particular) shall also have sufficient strength so that these systems cannot obtain unauthorised system and data access to the Middleware or the ECM/Long-Term Storage and its data.[83]
- The business applications connected to the Middleware shall pass a personal authentication and authorisation. In this way, only technically authorised persons should have access to the Middleware.

Failed authentication attempts shall be logged. It is to be considered from a technical perspective if access should be blocked after multiple failed authentication attempts, because this can also be used relatively easily for denial-of-service attacks.

Successful authentications may be logged.

[82] E.g. the custom application or a certification service provider

[83] In this context, the XML-Adapter is considered to be an external component even though it is defined in this Technical Guideline. Thus, authentication between the XML-Adapter and the Middleware shall be carried out. Furthermore, it shall be ensured that the XML-Adapter cannot be used by unauthorised business applications.

Any communication between the components of the Middleware and external applications or service providers (for example trust service providers) should be encrypted. If it is impossible to physically secure a communication relationship, the communication should be encrypted.

If an external service provider does not offer an option to encrypt the communication, it shall be checked whether another service provider that offers an encryption option can provide these services with the same quality.
Sufficiently strong encryption procedures and key lengths are to be used for the encryption of communication. The negotiation of a key strength that is inadequate or non-existent upon session start-up shall be prevented. Communication with too weak encryption shall not take place. The event shall be logged.

Communication is only initiated when necessary and only by the component set up for this purpose or the persons authorised to do so. Inquiries for a communication connection that are unfounded or unexpected shall be denied by all of the components.

Access to the log data of Middleware shall also be kept as restrictive as possible.

If the TR-ESOR-Middleware offers multi-client capable operation, the TR-ESOR-Middleware shall reliably prevent cross-client access to the archival information packages. In the case of high requirements for confidentiality, the TR-ESOR-Middleware should also be examined for covered channels and other attack vectors regarding possible breached of confidentiality.

If multi-client capable operation of the TR-ESOR-Middleware is necessary, these clients should also be continued consistently in the ECM/Long-Term Storage used.

8.2.3 Measures for the protection of authenticity, integrity and binding character

If securing the authenticity and integrity of electronic data with the help of digital signatures or time-stamps (i.e. time-stamp pursuant to **[eIDAS, Article 3(33)** and **34)]** is standardised or desired, digital signatures or time-stamps pursuant to **[eIDAS, Article 3(33)** and **34)]** of data and documents in sufficient quality shall generally be realised by the applications and before storage in the ECM/Long-Term Storage.

In order to ensure that no ambiguity arises during the hash value computation and also the digital signing of content data in XML notation, it is recommended that the content data is canonicalised prior to the computation of the hash value or digital signing. More information in this respect can be found in Annex TR-ESOR-M.2 Cryptographic-Module and TR-ESOR-M.3 ArchiSig-Module .

The digital signatures or time-stamps pursuant to **[eIDAS, Article 3(33)** and **34)]** are to be connected with the data cryptographically signed in such a way that the relationship between the digital signatures or electronic time-stamps pursuant to **[eIDAS, Article 3(33)** and **34)]** and the data cryptographically signed may also be reproduced by third parties at all times and without any doubt.

Furthermore, the validation data needed for a complete validation of the digital signatures or electronic time-stamps pursuant to **[eIDAS, Article 3(33)** and **34)]** should be obtained during or immediately after the creation of the digital signature or electronic time-stamp pursuant to **[eIDAS, Article 3(33)** and **34)]** and should also be connected with the digital signatures or electronic time-stamps and data cryptographically signed prior to the storage in the ECM/Long-Term Storage. This validation data shall be obtained by the ArchiSafe-Module at the latest upon storage in the archive system.

Thus, it is recommended that at least the digital signature data or electronic time-stamp data is stored together with the signature or seal or time-stamp validation data and the content data in an XML-based archival information package (see Annex **[TR-ESOR-F]** and **[TR-ESOR-ERS]**).

(A8.2-1) In order to guarantee the long-term verifiability of the digital signatures or electronic time-stamps, the digital signatures or electronic time-stamps and signature or seal or time-stamp validation data (certificates and status inquiries/-information) shall be deposited in standardised data formats. Details can be found in **[TR-ESOR-F]** or **[TR-ESOR-ERS]**.

(A8.2-2) If the information package to be archived is available in an XML format, this archival information package shall be verified for syntactic correctness by the ArchiSafe-Module against an XML schema file that has been stored in this component and authorised by the custom application. If this verification fails, the requirement (A5.1-4)0 is to be fulfilled.

(A8.2-3) If the archival information package to be archived includes digital signatures or electronic time-stamp and technical evidence records, if any, the ArchiSafe-Module shall verify the validity of the digital signatures or electronic time-stamps and technical evidence records as well on base of the shell model as on base of the chain model (or have it verified) and enter the validation results in a standardised form in the archival information package. If this verification fails for both validation methods (shell model and chain model), the he requirement (A5.1-5) is to be fulfilled.

(A8.2-4) If the verification is successful, the ArchiSafe-Module may provide the entire archival information package with an additional advanced electronic signature or seal or an electronic time-stamp.

(A8.2-5) All hash values in the ArchiSig-Database that do not have integrity protection yet shall be secured regularly by means of a qualified time-stamp pursuant to **[eIDAS, Article 42]** as an "archive time stamp" pursuant to the IETF's ERS standard described in more detail in Annex **[TR-ESOR-M.3]** "ArchiSig-Module".[84]

- Recommendation: at least once per day.

(A8.2-6) In a timely manner before the algorithms and parameters used for the archive time stamp[85] lose their suitability as security measures or it becomes known[86] that they are vulnerable, the content of the time-stamp field of the last (previous) archive time stamp shall be new hashed and a new archive time stamp calculated. This new time-stamp is based on algorithms suitable as security measures and shall be added to the ArchiSig-Database.

(A8.2-7) In a timely manner before the algorithms and parameters used for the calculation of the hash values of the archival information packages lose their suitability as security measures or it becomes known that they are vulnerable, new hash values shall be calculated for all these archival information packages in the ECM/Long-Term Storage on the basis of algorithms and parameters that are suitable as security measures and shall be secured with new archive time stamps pursuant to the IETF ERS standard **[RFC4998]** or **[RFC6283]**. The ECM/Long-Term Storage shall make efficient, secure and reliable access available to the ArchiSig-Module for this operation.

Because this operation could require a significant amount of time depending on the volume of data stored, the Middleware should maintain a secondary ArchiSig-Database parallel to the primary database as a fall-back solution. This secondary database shall use different cryptographic algorithms and parameters than the primary database. The secondary database shall secure exactly the same information packages as the primary database and be able to be put into operation at all times parallel to the primary database.

ArchiSig-Databases shall not be deleted or otherwise lost. This even applies if individual archival information packages have already been deleted or if the algorithms that were used have expired or have been breached.

The ArchiSig-Databases shall be kept on or in storage (media)[87] that make the basic mechanisms for securing integrity available. This not only applies to the time-stamps and hash values and to the archive data object IDs themselves, but also to the links between these data elements.

---

[84] An "archive time stamp" can be applied to an individual information package or to a group of information packages. The cryptographic representatives (hash values) of the individual information packages or groups of information packages are first summarised in a so-called Merkle hash tree **[MER 1980]** and the last hash value of the tree is then furnished with an initial time-stamp. In this manner, all hash values subsumed in a hash tree are first protected cryptographically with only one initial time-stamp (see also TR-ESOR-M.3 and http://www.ietf.org/rfc/rfc4998.txt).

[85] This includes both the hash procedures and the signature procedures.

[86] The time it becomes known is a corresponding entry in the algorithm catalogue of the Federal Network Agency.

[87] It is not required that the long-term storage system makes these mechanisms available. The ArchiSig-Module could also realise them itself.

The ECM/Long-Term Storage shall be chosen in such a way that a reproduction of the archival information packages (L)XAIP) and in case of LXAIP also the referenced external archive data objects stored or the ASiC-AIP and of the ArchiSig-Databases that is exact down to the last bit can be guaranteed.

All media (also backup media) held in the ECM/Long-Term Storage as well as the data stored on them shall be checked regularly for readability. Even if only minor errors are identified (e.g. bit errors on the medium), the corresponding medium shall be replaced or the databases affected shall be restored from integer backup media.

All components of the Middleware and the ECM/Long-Term Storage shall be designed in such a manner that parallel access to one or several different business applications, even those with different computing power and bandwidth use, does not result in undesired falsification of the transferred or stored data.

The cryptographic evidence records in the storage system shall be protected against unauthorised (write) access. In, particular, it shall also be ensured that administrator and user accounts for the archival information packages do not have any access to the evidence record databases. To do so, it is recommended that at least the logical separation of these two databases is maintained.

8.2.4 Measures for the protection of availability

Archival information packages may only be deleted if the defined minimum period of retention has expired and an order for deletion includes a reason for the premature deletion in the event of premature deletion. In the event of premature deletion, the reason shall be logged by the ECM/Long-Term Storage in a traceable manner and kept in an unadulterated manner for the duration of the retention periods (which relate to the deletion log, not the original document).
It is recommended that the double verification principle or another model for authorisation and control is enforced within the business application for (premature) deletion.[88]

The ECM/Long-Term Storage should store all data in a redundant manner. The concrete IT security concept shall show the degree to which this is necessary. This applies to both the actual archival information packages and the ArchiSig-Database.

The infrastructure and the technical components of the entire archive system and the connections to the external components shall have adequate availability and, if necessary, be designed in a redundant manner. The concrete IT security concept shall show the degree to which this is necessary.

All components of the Middleware shall be designed in such a way that none of the connected business applications can block access to the Middleware or the ECM/Long-Term Storage.

All components of the Middleware shall be designed in such a way that none of the Middleware-internal actions can block immediate access for the business applications.

8.2.5 Measures for authorisation

The business applications connected to the Middleware shall implement a reliable authentication and authorisation system that only allows authorised persons to access the Middleware.

For each archive request, the ArchiSafe-Module shall be able to verify whether the business application making the request is authorised to access the Middleware (in order to store, update, retrieve or delete data or verify supplemental evidence data and technical evidence records) .

The ArchiSafe-Module shall be able to verify whether the business application making the request is authorised to access (update, retrieve, delete or verify supplemental evidence data and evidence records) the archival information package identified by an AOID.

The ArchiSafe-Module shall be able to verify whether an archive request (e.g. store, update, retrieve, delete etc.) is a permissible command.

[88] In the government agency environment, other regulations shall be observed.

9. Conformity and interoperability

This chapter explains the conformity levels stipulated for this Technical Guideline and the procedure used to demonstrate proof of this conformity.

Notice: This chapter 9 will be revised in the context of TR-ESOR V1.3.

9.1 Conformity and conformity evaluation

Three levels that build on one another are stipulated for the conformity evaluation of individual modules or entire systems (see **[HKS 12]**).

These three conformity levels differ with regard to technical detail specifications of the interfaces and formats.

Products and systems that want to be certified pursuant to the Technical Guideline 03125 TR-ESOR shall prove their conformity pursuant to the corresponding available test specifications.

In order to be certified pursuant to the desired conformity level, a product or a system shall fulfil all MUST (or synonymously SHALL) conformity criteria (MUST test cases) for this conformity level and for all lower conformity levels.

A component or a system conforms to the Technical Guideline if the component or the system has passed required conformity evaluation without any deviation from the specifications applicable to the respective conformity level.

A conformity evaluation that has been passed successfully is the proof that the component or the system has fulfilled the technical requirements of this Technical Guideline.

A system to be verified may conform to all requirements or only implement the requirements of individual modules.

With respect to the levels of conformity, the following must be noted:

9.1.1 Conformity level 1 - Functional conformity

A system or a component functionally conforms to this Technical Guideline if the system or the component can be mapped functionally to the system composition described in this Technical Guideline or to individual (also several) modules of this system composition and compliance with the requirements (Ax.y-z) for the overall system or for individual modules is determined.

Functional conformity in the sense of this Technical Guideline means that the components fulfil the functional and security-related requirements defined in this Technical Guideline, the logical mapping of the functional requirements is presented in a comprehensible manner and the components can work with each other in a purposeful manner on the basis of the goals and standards listed in this Technical Guideline.

Functional conformity in the sense of this Technical Guideline does not mean that only XML-based archival information packages may be used for the storage in the ECM/Long-Term Storage.

Functional conformity in the sense of this Technical Guideline does not mean that the interfaces of the component or the system have to conform exactly to the ASN.1 or XML specifications.

The primary goal of this conformity evaluation is to demonstrate proof that the module or the overall system functionally implements the corresponding share for the preservation of evidence. The corresponding test specifications for the logically functional conformity level 1 can be found in **([TR-ESOR-C.1])**.

9.1.2 Conformity level 2 - Technical conformity

A system or a component technically conforms to this Technical Guideline if, in addition to the proof of functional conformity, also the highest external S.x interface concerned pursuant to the IT Reference Architecture (see **[TR-ESOR-E]**, Figure 2) has been implemented on the basis of the eCard-API as

described in **[TR-ESOR-E]** and a defined XML data format (e.g. (L) XAIP or ASiC-AIP) and evidence record format[89] as well as verification report-format[90] are used for communication and storage.[91]

The primary goal of this additional verification is to demonstrate proof that a level of technical interoperability can be reached on the basis of a well-defined standard. This is relevant in particular if using open, interoperable and standardised data formats and manufacturer-independent interfaces pursuant to national[92] and international[93] standards is generally desired or if only individual modules are verified that are sold as stand-alone products and thus have to work with other modules/systems.

The verification of the technical conformity includes in particular:

1. The verification of the relevant highest external web service interface specified in **[TR-ESOR-E]**,
2. The verification of the syntactic and semantic correctness of the Evidence Records pursuant to **[RFC4998]** or **[RFC6283]**[94] and **[TR-ESOR-ERS]**,
3. The verification of the syntactic and semantic correctness of the (L)XAIP containers or ASiC-AIP,
4. The verification of the verification report in the form of a VerificationReport element pursuant to **[TR-ESOR-VR]**.

(L)XAIP or Delta-(L)XAIP as defined in **[TR-ESOR-F]** should be used as XML data format and ASiC-AIP as ZIP-Format. Deviations in the XML-/ZIP- data format used are permissible, but it shall be explained that equivalent functionality is supported. It shall be explained in particular how a transformation into the (L)XAIP or ASiC-format as specified in Annex **[TR-ESOR-F]** can be performed.

The corresponding test specifications for the logically functional conformity level 2 can be found in **([TR-ESOR-C.2])**.

9.1.3 Conformity level 3 - Conformity with the German Federal Agency Profiling

The test cases of conformity level 3 are based on the additional requirements pursuant to Annex **[TR-ESOR-B]**.

The corresponding test specifications for conformity level 3 Conformity with the German Federal Agency Profiling can be found in **([TR-ESOR-C.3])**.

89 RFC 4998 shall, RFC 6283 may be supported.

90 See [TR-ESOR-VR]

91 It is to be noted here that trivial XML data formats that merely encapsulate a proprietary format are not allowed. XAIP as defined in Annex **[TR-ESOR-F]** should be used as XML data format. Deviations in the XML data format used are permissible, but it shall be explained that equivalent functionality is supported. It shall be explained in particular how a transformation into the XAIP format as specified in Annex **[TR-ESOR-F]** can be performed.

92 SAGA, XÖV, ArchiSafe

93 MoReq2, OASIS

94 RFC 4998 shall, RFC 6283 may be supported.

9.2 Entities participating in the conformity evaluation

The following entities participate in a conformity evaluation:

Applicant	Manufacturer, distributor or operator of a component/ system in the sense of this Technical Guideline.
Target of the evaluation	Component/system pursuant to this Technical Guideline that is provided for the conformity evaluation.
Testing body	A body or institution that has been accredited by BSI and carries out the conformity evaluation.
Confirmation body	Conformity confirmation body of the BSI.

9.2.1 Applicant

The applicant would like to have the conformity of their system or their component(s) verified and confirmed pursuant to one of the conformity levels of this Technical Guideline that are listed above.

To do so, the applicant applies for a confirmation of the conformity of their system or their component(s) at the BSI. The official application date is essential for the processing sequence of the different confirmation procedures performed at the BSI. The applicant is informed by the BSI when the application has been received in full and the procedure number has been issued.

The applicant concludes a contract with the testing body for the implementation of the conformity evaluation.

The applicant is obligated to provide all information needed for the implementation of the conformity evaluation, the target of the evaluation itself and, if applicable, any required evaluation tools and training measures. They are responsible for the correctness of the information provided about their system or their component(s).

9.2.2 Target of the evaluation

The system or the component the conformity of which is to be confirmed is referred to as a target of the evaluation.

This may be a software product that runs on a certain platform and is to be used in a certain environment of use. It may also be a hardware product or a combination consisting of software and hardware products.

At the time the conformity evaluation is carried out, the target of the evaluation shall be completely available and the development shall have been completed for the version submitted for evaluation. The version of the target of the evaluation is documented when the application is made.

Improvements to the target of the evaluation during the conformity evaluation are only possible in consultation with the BSI.

9.2.3 Testing body

Conformity evaluations with the goal of confirmation by the BSI are carried out by the testing bodies that have been accredited by the BSI.

Compliance with DIN EN ISO/IEC 17025 is a prerequisite for accreditation.

The testing body is responsible for the correctness of their evaluation results and documents these results in an evaluation report. The conformity evaluation is only carried out after an application for conformity has been officially accepted by the BSI. To do so, the testing body actively consults the confirmation body of the BSI with regard to the planning and implementation of the conformity evaluation. This consultation includes the scheduling, the planning of the technical implementation and information about the evaluators to be used in the procedure.

The evaluation report documents the progress of the evaluation as well as the results. It is presented to the confirmation body for evaluation and acceptance. The applicant receives the final evaluation report after it has been accepted by the confirmation body of the testing body.

The testing bodies accredited by the BSI and the BSI have concluded a contract that regulates their respective rights and obligations.

The approved testing body is obliged to treat the manufacturer information and the targets of the evaluation as well as the results of the evaluations in a confidential manner and to protect them against unauthorised disclosure. The need-to-know principle shall be applied. Confidentiality shall be maintained in the communication with the confirmation body. All evaluation documents are to be labelled as "company confidential" documents.

Manufacturer information and evaluation reports shall be subject to a configuration management in the testing body.

The service provided by the testing body shall be integrated into the testing body's quality management system.

Accredited testing bodies are published by the BSI in regularly updated publications and are available on the BSI website.

9.2.4 Confirmation body

The task of the confirmation body is to monitor the progression of the conformity evaluation (accompany the evaluation) and to prepare the conformity report and the notice of conformity after the evaluation has been carried out successfully.

The confirmation body evaluates the application for the confirmation of conformity. When the implementation of the evaluation is coordinated by the testing body listed in the application, the information of the testing body about the scheduling, planning of the technical implementation of the evaluation and, if applicable, the information about the skills and expertise of the evaluators mentioned are evaluated. If applicable, questions with regard to licences as well as skills and expertise are clarified with the accreditation body of the BSI.

After the evaluation of the application has been completed, the applicant and the testing body are informed of the official application date and the procedure number. The procedure number is the process identification code at the BSI. It is used for each piece of correspondence in order to label the documents and the confirmation documents.

The confirmation body of the BSI or an employee of the BSI commissioned by the confirmation body participates in parts of the implementation of the technical conformity evaluation if necessary. The evaluation report presented by the testing body is evaluated, commented on if necessary and accepted.

To complete the evaluation procedure, the confirmation body prepares a certificate as well as the associated notice of conformity.

Confirmed products and systems are published by the BSI through the confirmation body provided that the applicant agrees to this.

9.3 Processing the conformity evaluation

Conformity evaluations are carried out by a testing body. During the conformity evaluation, the targets of the evaluation go through the following three successive phases:

1. Preliminary phase
2. Carrying out the conformity evaluation
3. Confirmation of conformity

9.3.1 Preliminary phase

The first phase consists of the following steps:

- Application for conformity evaluation submitted by the applicant by indicating the conformity level

- Evaluation of the application by the confirmation body
- Official acceptance of the application by the BSI
- Coordination of the implementation of the evaluation by the parties
- Provision of the target of the evaluation and the documents required pursuant to this Technical Guideline by the manufacturer/operator.

9.3.2 Carrying out the conformity evaluation

In the second phase, the selected and parametrised evaluation sequence is implemented by the testing body. Depending on the evaluation method, different evaluation procedures or evaluation tools are used. The evaluation results that arise during the evaluation are collected and archived in a suitable manner. Furthermore, the evaluation results that are generated and observed during the implementation of the evaluation are analysed and documented and an evaluation report is prepared. The conformity evaluation consists of the following steps:

- Implementation of the technical evaluation by the testing body pursuant to the specifications of this Technical Guideline and pursuant to the planning and implementation coordinated with the confirmation body; if necessary, supervisory on-site support by the BSI during the evaluation in order to ensure consistent procedures and methods and, if applicable, assessments that can be compared with each other
- Documentation of the individual steps of the implementation and the results of the evaluation in an evaluation report by the testing body
- Evaluation, commenting if necessary and acceptance of the evaluation report by the BSI.

During the evaluation, it is checked whether all "shall"[95] requirements have been fulfilled completely. Deviation from the "shall" requirements is not allowed.

Furthermore, all "should" requirements are also evaluated. If they are not complied with, the applicant shall provide the reasons for this in writing in a coherent and comprehensible manner.

"may" requirements are not the subject of the evaluation.

9.3.3 Confirmation of conformity

This phase includes:

- Preparation of the conformity report and the certificate and issuance of the notice of conformity by the BSI,
- Publication of the results provided that the applicant has agreed to this.

9.4 Interoperability

Whereas the conformity evaluation determines whether the implemented components conform to the functional requirements of this Technical Guideline, interoperability between conforming components means that these components can work together on a technical level.

Thus, the functional conformity is the prerequisite for the interoperability, but it is not always sufficient. If functional conforming components each fulfil different requirements of a specification that do not have a common intersection, then the components each individually functionally conform to the specification, but are not interoperable with each other.

In the scope of this Technical Guideline, no separate interoperability evaluations are carried out for the functional conformity evaluation, but the criteria for conformity are determined in such a suitable manner that the components have been designed logically and functionally interoperable.

For the technical interoperability evaluation, comprehensible technical proof shall be provided to demonstrate that the evaluated components or modules have correctly implemented the interfaces specified with the help of the eCard-API.

[95] Of course, these evaluations also relate to all those requirements that are designated with the term "is", "shall not" etc.

10. Annexes

This Technical Guideline includes this Main Document and, pursuant to the Reference Architecture recommended in chapter 7, the following annexes regarding the modules (components) and interfaces defined in the IT Reference Architecture.

10.1 TR-ESOR-M.1 ArchiSafe-Module

The annex with the designation "TR-ESOR-M.1 ArchiSafe Module" specifies and explains the functional and security-related requirements for a secure gateway that regulates the flow of information within the Middleware and thus, related to this, also the access to the ECM/Long-Term Storage for the following operations:

- Storing archive data objects
- Updating archival information packages (optional)
- Retrieving archival information packages (in whole or in part)
- Retrieving technical evidence records
- Verifying supplemental evidence data and technical evidence records (optional) and
- Deleting archival information packages.

The goal of the ArchiSafe-Module is the realisation of a strict logical separation of the upstream IT custom applications from the actual ECM/Long-Term Storage systems. When storing digitally signed or timestamped data and documents, the ArchiSafe-Module also secures the probative value of the information to be archived by means of the following operations:

1) Electronic signatures, seals or time-stamps and if applicable, further supplemental evidence data (certificates, certificate revocation lists, OCSP responses, etc.) and technical evidence records (Evidence Records) are verified for their validity and the verification results are embedded or stored otherwise in the XML documents in a standardised form. The signature, seal or time-stamp validation and if applicable, the validation of further supplemental evidence data and technical evidence are realised by a Cryptographic-Module that shall fulfil the requirements described in Annex TR-ESOR-M.2. The interface between the ArchiSafe-Module and the cryptographic devices is specified in Annex TR-ESOR-S (see "S.1 interface" in this document).
2) The ArchiSig-Module which is responsible for preservation of evidence methods, e.g. by signature, seal or time-stamp renewal (see Annex TR-ESOR-M.3) returns the archive data object ID (AOID) after the calculation of the hash value which is carried out there has been completed. Access to the archival information package at a later point in time is only possible with this AOID.

Furthermore, this module offers standardised interfaces for the communication with the cryptographic components (TR-ESOR-M.2 and TR-ESOR-M.3) that support the preservation of the evidence of the electronic documents stored.

Every archive request from an upstream, external IT application for storing, updating or retrieving archived data and documents in or from the ECM/Long-Term Storage with the additional goal of preserving evidence shall be carried out through the ArchiSafe-Module.

For this purpose, the external IT application opens a secure communication channel with the ArchiSafe-Module and sends an archive request. The ArchiSafe-Module identifies and authenticates the application making the request and verifies the syntactic validity of the archive request being transmitted by the application making the request against the configuration data stored in the ArchiSafe-Module (XML schemata, communication and processing rules).

10.2 TR-ESOR-M.2 Cryptographic-Module

The annex with the designation "TR-ESOR-M.2 Cryptographic-Module" specifies and explains the functional and security-related requirements for Cryptographic-Modules for hash calculation, the

validation of electronic signatures, seals or time-stamps and for obtaining of qualified time-stamps and (optionally) electronic signatures or seals.

The Cryptographic-Module provides the cryptographic functions that are needed for the preservation of evidence in a centralised manner by itself or by request from a Trust Service Provider. These functions primarily include cryptographic procedures required for the validation of technical evidence records and supplemental evidence data, for example electronic signatures, seal or time-stamps and the computation of hash values.

The Cryptographic-Module has the following cryptographic functions; it does not implement any **business** processes:

- Cryptographic functions:
    - Validation of digital signatures (by itself or by request from an external Trust Service Provider)
    - Validation of electronic certificates up to a trustworthy root certificate (by itself or by request from a Trust Service Provider)
    - Computation of a hash values of electronic data submitted
    - Requesting qualified time-stamps by request from a qualified Trust Service Provider
    - Validation of a (qualified) time-stamps (by itself or by request from a qualified Trust Service Provider
    - Requesting digital signatures (electronic signatures or seals) from a trust service provider (optional)

Furthermore, the Cryptographic-Module describes basic requirements for the algorithms used, the Canonicalization of XML-objects as well as the required security functionalities and the configuration of the Cryptographic-Module.

10.3 TR-ESOR-M.3 ArchiSig-Module

The annex with the designation "TR-ESOR-M.3 ArchiSig-Module" explains the functionalities and the security-related requirements of a Cryptographic-Module for the preservation and renewal of the probative value of electronic signatures, seals or time-stamps pursuant to the IETF's ERS standard (**[RFC4998]** or **[RFC6283]**)[96].

Cryptographic operations such as electronic signatures, seals or time-stamps only make it possible to prove the integrity or authenticity of electronic data if the algorithms on which the signatures,seals or time-stamps are based are suitable as security measures from a mathematical and technical perspective. Durable and verifiable preservation of authenticity and integrity of electronic data thus makes the use of additional security measures necessary that make it possible to prove that digitally signed or time-stamped data in particular were stored in an unaltered manner for the duration of the retention periods.

The task of the ArchiSig-Module is the preservation of the evidence by means of additional cryptographic securing measures and the generation and return of evidence records.For this purpose, the ArchiSig-Module implements a cryptographic solution that ensures in particular that the procedure for maintaining the security and trustworthiness of electronic signatures, seals or time-stamps standardised in § 15 of the German Trust Service Act **(**Vertrauensdienstegesetz **[VDG, § 15])**[97] can be fulfilled by appropriate means of preservation of evidence, for example by a renewal of a qualified electronic time-stamp, in a reliable and economic manner, i.e. also for larger amounts of data.

The renewed qualified electronic time-stamp pursuant to **[eIDAS, Article 42]** contains a renewed digital signature and shall include the data and the earlier electronic time-stamps with their digital signatures and be created with cryptographic algorithms and parameters that are suitable as security measures.

[96] RFC 4998 shall, RFC 6283 may be supported.

[97] See also **[ETSI SR 019 510], [ETSI TS 119 511]** and **[ETSI TS 119 512].**

The signature renewal procedure may be automated and set up so that many documents are newly digitally signed or time-stamped together.

The renewed qualified electronic time-stamps pursuant to **[eIDAS, Article 3(34)** and **Article 42] each in accordance** with a digital signature on the basis of qualified certificates are issued on request by qualified Trust Service Providers with the status "granted" pursuant to **[eIDAS, Article 3(17)** and **Article 24]**.

The basis of the ArchiSig-Module is the IT implementation of the IETF's Evidence Record Syntax (ERS for short) standard ([**RFC4998]** or **[RFC6283])**. ERS defines in detail how suitable procedures of preservation of evidence can be carried out automatically for large amounts of documents. Furthermore, the standard defines the data formats in which the technical evidence records are provided and exchanged for an unlimited period of time. Aspects with regard to data protection are also taken into account because it is also possible with the ERS standard to delete parts of the document database without compromising the conclusiveness of the remaining parts.

Technically, the ERS standard is based on the approach that cryptographic checksums (hash values) of the archival information packages are saved as a cryptographically unique representative of the data to be stored when the data is deposited in the ECM/Long-Term Storage together with a qualified archive time stamp.

10.4 TR-ESOR-S Interface Specifications

The annex with the designation "TR-ESO**R-S" V1.1.1 is historical and will not be developed further on. It is replaced by [TR-ESOR-E].**

10.5 TR-ESOR-ERS Evidence Record Profiling pursuant to RFC4998 and RFC6283

The Annex ERS "Evidence Record Profiling pursuant to **[RFC4998]** or **[RFC6283]**" specifies an interoperability profile for technical evidence records (Evidence Records) pursuant to **[RFC4998]** or **[RFC6283]**. This profile is to ensure a long-term and largely system- and platform-independent interpretability of Evidence Records between different TR-ESOR implementations.

This annex stipulates the primary criteria for the evaluation of the technical *conformity*.

10.6 TR-ESOR-VR Verification Reports for Selected Data Structures

The Annex VR "Verification Reports for Selected Data Structures" describes and specifies the verification reports for an archival information package and, if applicable, also for the associated technical evidence records. At the moment, this annex is only available in English. The translation into German is planned.

This annex stipulates the primary criteria for the evaluation of the technical *conformity*.

10.7 TR-ESOR-F Formats

The annex with the designation "TR-ESOR-F Formats" (**[TR-ESOR-F]**) specifies, using the `<XAIP>` element, an XML-based container format for archival information packages (XAIP) ((XAIP) pursuant to (**[TR-ESOR-F]**, clause. 3.1) or a logical XAIP (LXAIP) pursuant to (**[TR-ESOR-F]**, clause 3.2, (i.e. a variant of XAIP, where there may be a reference to externally stored data objects in the ECM/Long-Term Storage) or an an ASiC-AIP pursuant to (**[TR-ESOR-F]**, clause 3.3) that is generated and processed by Middleware components that conform to this Technical Guideline and, using the `<DXAIP>` element, a Delta-XAIP or Delta-LXAIP-structure submitted during the `ArchiveUpdateRequest` (see TR-ESOR-E).

Furthermore, Annex F (**[TR-ESOR-F]**) specifies and explains the functional and security-related requirements for data formats for depositing payload data, meta information and signature data (archival information packages). Moreover, the formats recommended for the communication with external systems and partners, such as the Trust Service Providers, are also explained in this document.

10.8 TR-ESOR-B German Federal Agency Profiling

The Annex B "German Federal Agency Profiling" specifies requirements, data formats and protocols for the storage of cryptographically signed data and documents with preservation of evidence for federal administration issues in particular.

"This profile should at least be applied by German federal agencies when the new procurement or update of an archive system or an Archive-Middleware for the storage of cryptographically signed documents is scheduled. For already existing installations which are to be used to store cryptographically signed documents for a long period of time, applying this profile is highly recommended" (see **[TR-ESOR-B]**).

10.9 TR-ESOR-E Concretisation of the Interfaces on the Basis of the eCard-API-Framework

The Annex E “Concretisation of the Interfaces on the Basis of the eCard-API-Framework” (**[TR-ESOR-E]**) includes an XML-based specification of the different functions for the preservation of evidence of cryptographically signed documents.

This annex provides the basis for the evaluation of ***technical conformity***. This document is not relevant to the "Functional conformity" level.

10.10 TR-ESOR-C.1 Conformity Test Specification (Level 1 - Functional Conformity)

The Annex C.1 "Conformity Test Specification (Level 1 - Functional Conformity)" describes and specifies the conformity test cases with regard to conformity level 1 "Functional conformity".

At the moment, this annex is only available in English. The translation into German is planned.

10.11 TR-ESOR-C.2 Conformity Test Specification (Level 2 - Technical Conformity)

The Annex C.2 "Conformity Test Specification (Level 2 - Technical Conformity)" describes and specifies the conformity test cases with regard to conformity level 2 "Technical conformity".

At the moment, this annex is only available in English. The translation into German is planned.

10.12 TR-ESOR-C.3 Conformity Test Specification (Level 3 - Conformity with German Federal Agency Profiling)

The Annex C.3 "Conformity Test Specification (Level 3 - Conformity with the German Federal Agency Profiling)" describes and specifies the conformity test cases with regard to conformity level 3 "Conformity with the German Federal Agency Profiling".

At the moment, this annex is only available in English. The translation into German is planned.

11. Table of abbreviations

AIP	Archival Information Package
AOID	Archive Data Object ID (Identifier)
API	Application Programming Interface
ARS	ArchiSafe Recordkeeping Strategy
ASCII	American Standard Code for Information Interchange
ASiC-AIP	Associated Signature Container (ASiC) Archive Information Package
ASN.1	Abstract Syntax Notation One
ATS	Archive Time Stamp
AZS	German: Archivezeitstempel, equivalent to ATS
BaFin	(German) Federal Financial Supervisory Authority
BArchG	(German) Federal Archiving Law
BDSG	(German) Federal Data Protection Act
BFH	(German) Federal Fiscal Court
BGB	(German) Civil Code
BGBl	(German) Federal Law Gazette
BGH	(German) Federal Court of Justice
BMF	(German) Federal Ministry of Finance
BMI	(German) Federal Ministry of the Interior
BMWi	(German) Federal Ministry of Economics and Technology
BNetzA	(German) Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway
BSI	(German) Federal Office for Information Security
BStBl	Federal Tax Gazette
CA	Certification Authority
CC	Common Criteria for Information Technology Security Evaluation
CCITT	Comité Consultatif International Téléphonique et Télégraphique
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DIN	German Institute for Standardization (Deutsches Institut für Normung)
DOMEA	Document Management and Electronic Archiving in IT-Supported Transaction (Dokumentenmanagement und elektronische Archivierung im IT-gestützten Geschäftsgang)
DSS	Digital Signature Standard
DSSC	Data Structure for Security Suitability of Cryptographic Algorithms
DTD	Document Type Definition
DXAIP	Delta-XAIP-Archival Information Package
DLXAIP	Delta-LXAIP-Archival Information Package
ECM	Enterprise Content Management
eIDAS-DG	Gesetzes zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Durchführungsgesetz)
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC)
(EU)910/2014	A synonym for eIDAS: eIDAS-Regulation (EU) No 910/2014, see above

ERS	Evidence Record Syntax
ETSI	European Telecommunications Standards Institute
EuGH	European Court of Justice
GDPdU	Principles of Data Access and Auditability of Digital Documents (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen)
GoB	Principles of Orderly Bookkeeping (Grundsätze ordnungsgemäßer Buchführung)
GoBS	Principles of Orderly IT-Supported Bookkeeping Systems (Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme)
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IPSec	Internet Protocol Security
ISIS-MTT	Industrial Signature Interoperability Specification-Mailshot
ISO	International Organization for Standardization
IT	Information technology
ITSEC	Information Technology Security Evaluation Criteria
JPEG	Joint Photographic Experts Group
LDAP	Lightweight Directory Access Protocol
LXAIP	logical XAIP pursuant to **([TR-ESOR-F], clause 3.2)**
(L)XAIP	XAIP pursuant to **([TR-ESOR-F], clause 3.1)** or LXAIP pursuant to **([TR-ESOR-F], clause 3.2)**
MIME	Multi-Purpose Internet Mail Extension
NIST	National Institute of Standards and Technology (USA)
No.	Number
OAIS	Open Archival Information System
OCSP	Online Certificate Status Protocol
ODF	Open Document Format
OSCI	Online Service Computer Interface
PDF	Portable Document Format
PK-DML	Document Management Certification Criteria (Prüfkriterien für Dokumentenmanagement-Lösungen)
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PKIX	PKI Working Group of the IETF
PNG	Portable Network Graphics Format
PP	Protection Profile
RFC	Request for Comments
S/MIME	Secure Multi-Purpose Internet Mail Extension
SAGA	Standards and Architectures for E-Government Applications (Standards und Architekturen für E-Government-Anwendungen)
SASL	Simple Authentication and Security Layer
SCVP	Server-Based Certificate Validation Protocol
SigG	(German) Signature Act
SigV	(German) Signature Ordinance
SMTP	Simple Mail Transfer Protocol
SNIA	Storage Network Industry Association
SR	Special Report
SSL	Secure Sockets Layer (Protocol)

ST	Security Target
TAP	Trustworthy Archival Protocol
TC	Trust Center
TCP/IP	Transmission Control Protocol / Internet Protocol
TIFF	Tagged Image File Format
TLS	Transport Layer Security
TS	Time Stamping
TSP	Trust Service Provider
UML	Unified Modeling Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
VDG	Trust Service Act (German: Vertrauensdienstegesetz (VDG)
WWW	Word Wide Web
XAIP	XML-formatted Archival Information Package
XML	eXtensible Markup Language
XSD	XML Schema Definition
ZDA	Certification Service Provider
ZPO	(German) Code of Civil Procedure

12. Glossary

Sender	An external (upstream) IT application (client software) that transfers data for archiving to the archive system.
Abstract Syntax Notation One (ASN.1)	The Abstract Syntax Notation One (ASN.1) makes it possible to describe the syntax of data accurately and independently of the actual coding. It was developed as part of the **[X.408]** standard and then standardised in [**X.680].**
Prima Facie Evidence (German: Anscheinbeweis)	There is prima facie evidence if a circumstance that is taken for granted as a fact of life suggests a certain (typical) course of events for a circumstance related to it, and thus appears to prove it indirectly. Prima facie evidence is possible in the case of typical event sequences. If there is a circumstance which suggests a certain course of events based on all experience of daily life, then this course of events can be considered proven. The prima facie evidence is not legally regulated. However, the law sometimes refers to prima facie evidence in individual cases (such as § 371a of the German Code of Civil Procedure (**[ZPO]**) for qualified electronic signatures).
ArchiSafe	In the scope of the e-government project of the German federal government "ArchiSafe Evidence Preserving Long Term Archiving of Electronic Documents", the basis for a cost-effective and scalable electronic archiving solution, has been defined and implemented in the form of a pilot scheme. The IT concepts developed during the project make it possible to electronically store digital documents permanently in a secure manner. The project intentionally ties in with the results of the project "ArchiSig – Long-Term Archiving of Digitally Signed Documents" in which the main basis of archiving →cryptographically signed documents with preservation of evidence has been developed. For more information, see http://www.archisafe.de. In the scope of this Technical Guideline, the term "ArchiSafe-Module" refers to a single, functional archive interface component that ensures strict logical separation of upstream IT applications from the actual long-term storage systems and thus is able to prevent unauthorised access to the long-term storage system in a reliable manner.

ArchiSig

ArchiSig is a joint project promoted by the German Federal Ministry of Economics and Technology (BMWi) in the scope of the "VERNET – Secure and Reliable Transactions in the Public Communication Networks" program for the conclusive and secure long-term storage of →cryptographically signed documents. In the scope of the ArchiSig project, concrete legal requirements to be fulfilled by a system for the long-term storage of →cryptographically signed documents were derived from the general statutory regulations and implemented prototypically. It was possible to show for the first time that the long-term storage of →cryptographically signed documents can be performed in a manner that complies with the law, is efficient and acceptable.

For more information, see

https://www.uni-kassel.de/fb07/fileadmin/datas/fb07/5-Institute/IWR/Ro%C3%9Fnagel/projekte_abgeschlossen/projekt_ArchiSig.pdf.

In the scope of this Technical Guideline, the term "ArchiSig-Module" describes a cryptographic solution that ensures the ability to prove the authenticity and integrity, and thus the probative value of →cryptographically signed documents in particular by means of additional cryptographic security measures in compliance with the legal requirements. For this purpose, the ArchiSig-Module implements a cryptographic solution that ensures in particular that the procedure for maintaining the security and trustworthiness of electronic signatures, seals or time-stamps outlined in § 17 German Signature Ordinance (**[SigV]**), since 2017 replaced through § 15 of the → Trust Service Act (German: Vertrauensdienstegesetz **[VDG]**), in the context of the →German **"Law for Implementing the "Regulation (EU) No 910/2014""**, can be fulfilled by means of →digital signature or time-stamp renewal in a reliable and economic manner, i.e. also for larger amounts of data.

Archive Request

An XML-based message that is transferred from an authorised external application (client software) to the ArchiSafe-Module and initiates an→archive operation.

Archival Information Package (AIP)

An archival information package[98] in the sense of this Technical Guideline is a self-explanatory and well-formed XML document that can be verified against a valid and authorised XML schema.

Archiving, Electronic A.

The permanent and unchangeable storage (saving) of electronic documents and other data is generally referred to as "electronic archiving" in common language usage in the field of information technology. From an information technology perspective, the time horizon circumscribed using the term "permanent" is a period of time not specified in more detail in which significant, but generally hardly foreseeable technical or technological changes could take place that, among other things, could result in the information technology systems with which the documents were originally written, created and saved no longer being available. In the meantime, the term "electronic (digital) long-term storage" is used to highlight the difference compared to a short-term "living records filling" or backup.

From a legal perspective, the term "archiving" is specified by and reserved for the Federal and State Archiving Laws and shall therefore be differentiated from storage over a limited period of time. In a legally correct sense, archiving solely concerns government documents and refers to how the documents of a government agency are to be sorted out and preserved by a competent governmental facility (Archive) for an unlimited period of

[98] In some Annexes to the Technical Guideline 03125, the more specific technical term "data objects" is also used in some cases to refer to "information packages".

time as soon as they are no longer needed for the purposes of that agency (see §§ 1, 3 and 5 German Federal Archiving Law **[BArchG]**).

Archive Operation

First of all, an archive operation is the execution of defined functions (operations) in the TR-ESOR-Middleware. The execution of these functions, as a rule, is followed by a function in the long-term storage.

Archive Time Stamp

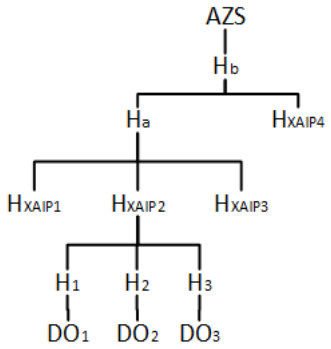
An archive time stamp is a time-stamp that, in connection with an digital signature, or seal confirms that certain data intended to be stored in the archive were present at a certain point in time. This is achieved in that the time-stamp refers to the →hash values of the corresponding data.

Pursuant to the eIDAS-Regulation (see →eIDAS-Regulation and →(**[eIDAS]**) a **qualified** electronic time-stamp pursuant to **[eIDAS- Article 42]** is signed or sealed either with an advanced electronic signature or with an advanced electronic seal of a qualified trust service provider or an adaquate procedure is used.

Pursuant to the ArchiSig concept, not each individual document has to have a time-stamp. Rather, it is sufficient to furnish at the root →hash trees that represent many documents with a qualified time-stamp, that includes a signature or seal.

The so-called "reduced hash tree" includes exactly the number of entries in this hash tree needed to prove the integrity of the document.

Example: The following hash tree:



Accordingly, the "reduced hash tree" for H_{XAIP2} consists of the sequence (H_1, H_2, H_3), (H_{XAIP1}, H_{XAIP3}), (H_{XAIP4}). The hash values H_{XAIP2}, H_a and H_b can be inferred from the delivered values and the proof of integrity can be kept with the AZS.

Asymmetrical Cryptographic Algorithms

For asymmetrical cryptographic algorithms, there is a complementary pair of keys (private key and public key) that can be used to realise electronic →signatures, →seal or →time-stamps for agreement on secret keys or encryption. The concept of asymmetrical cryptographic algorithms can be traced back to W. Diffie and M. Hellman **[DiHe 76].** The most common asymmetrical algorithm today is the RSA algorithm.

Authentication

Authentication serves to verify the identity of a user or a communication partner, or rather the source of a message. During the authentication, certificates of a trustworthy entity are used to determine the identity. Functions that create and send a cryptographically secured (signed or sealed) "fingerprint" of the uncoded original message serve to check the integrity (and authenticity) of a message.

Authenticity

Electronic →data is authentic if it corresponds to the original data and the identity of an issuer (author, creator and/or sender) can be assigned to it without any doubt.

German Federal Archiving Law (BArchG)

The **German Federal Archiving Law** or the Law on the Securing and Use of the Archive Material of the Federation in Germany determines how the archive material is to be secured, made usable, and utilised in a scientific manner in the long term.

In this context, archives are (governmental) institutions that take over the documents of all government agencies in their area of responsibility - thus all federal agencies in the case of the Federal Archive (= State Archive of the Federal Government and Federal Administration) - and assess, store and provide them for later use in the archive as soon as they are no longer needed for the purposes of the government agency at which they were created (§§ 1,3 and 5 **[BArchG]**). In this case, archiving does not occur for a long period of time, but rather for an unlimited period of time (permanently "for eternity"; see German Federal Archiving Law (**[BArchG]**), Commentary (Handkommentar), Baden-Baden 2006, § 1 marginal number 18).

BASE64

Base64 is a term used for encoding binary data in a character string that only consists of a few codepage-independent ASCII characters. The procedure is mainly used in the MIME (Multi-Purpose Internet Mail Extensions) Internet standard and is thus used for example when sending e-mail attachments. This is necessary to ensure smooth transport of any binary data, since SMTP in its original version was only designed for sending 7-bit ASCII characters.

For the encoding, three bytes of the byte stream (=24 bits) are divided into four 6-bit blocks. Each of these 6-bit blocks forms a number between 0 and 63, which also explains the name of the algorithm. On the basis of a conversion table, these numbers are converted into "printable ASCII characters" and output.

Due to this coding, the space requirements rise by approx. 36% (33% due to the encoding itself, another 3% due to line breaks).

Certificate

Certificates for →electronic signatures and →electronic seals are electronic certifications that are issued (signed) by a →Trust_Service_Provider with which certain information, especially a →public key, can be assigned to the certificate owner and that confirm “at least the name or the pseudonym of that person`` (**[eIDAS, Article 3(14)]**).

The most common format for certificates is X.509. In addition to the public key, the certificate particularly includes personal information that was verified by the issuing entity at the time the certificate was issued and information regarding the period of validity.

Certificate Path

A “certification path” is an “ordered list of one or more public-key certificates, starting with a public-key certificate signed by the trust anchor, and ending with the public-key certificate to be validated ”.

A certification path consists of a chain of certificates $Z1 - Z2 - \cdots - Zn$, in which case for all i from 1 to $n - 1$ the owner of $Zi+1$ issued the certificate Zi and Zn is the certificate of a trust anchor.

Certificate Policy (CP)

A certificate policy consists of a number of regulations that are taken into account upon the issuance of a certificate. It can be decided on the basis of a certificate policy whether a certificate offers sufficient security for a certain use. There is a framework for the development of Certificate Policies in **[RFC3647]**.

Certificate, qualified

Pursuant to (**[eIDAS, Article 3(15)]**) ”‘qualified certificate for electronic signature’ means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I;”

Certificate Revocation List	A revocation list is created by a a →Trust_Service_Provider pursuant to eIDAS-Regulation **[eIDAS]** and published in a →directory service. It contains information about which certificates were revoked by the certificate owner or other authorized authorities. A widely accepted format for revocation lists was specified in **[X.509]** and profiled in more detail in **[RFC3280],** obsoleted by **[RFC5280]**.
Evidence Records, technical	Evidence Records serve to prove the intactness of the integrity and authenticity of the archived information packages. In accordance with the specifications of the IETF's ERS standard, a set of evidence records includes a set of archive time stamps of sufficient quality about the stored (signed, sealed or timestamped) →archival information packages that prove the intactness of the data and additional information that prove the correctness and validity of electronic signatures, seals or time-stamps at the time of signing or sealing or timestamping as well as the timely signature or seal or time-stamp renewal pursuant to the legal requirements.
Supplemental Evidence Data	Supplemental evidence data are signatures or seals or time-stamps for exactly one information package or document and it also includes the verification data necessary for the verification of the signature or seal or time-stamp signature or time-stamp seal, such as certificates as well as CRL lists and OCSP responses to these certificates. The →evidence records prove that the document existed and was not changed anymore after being archived. Supplemental evidence data prove that the signatures, seals and time-stamps which may have been created outside of the archive are valid, or rather were valid at the time of creation.
Preservation of Evidence	In the sense of this Technical Guideline, preservation of evidence means that a system conforming to this Technical Guideline is able to maintain the probative value of the electronic information stored in it for the duration of the retention period and thus ensure the legal consequences intended by means of the storage of the electronic documents at least for the duration of the statutory retention periods. Technically, this is realised by means of →evidence records and →supplemental evidence data.
Preservation techniques	→Signature or seal or time-stamp renewal, optionally together with hash renewal pursuant to the Trust Service Act (German: Vertrauensdienstegesetz **[VDG]**) and **[ETSI SR 019 510], [ETSI TS 119 511]** and **[ETSI TS 119 512]**,
Client Software	An external (upstream) IT application that is capable and authorised to use the →ArchiSafe-Module to archive data in the long-term storage and search for, update, retrieve or delete archived data.
Common Criteria (CC)	With the Common Criteria for Information Technology Security Evaluation (Common Criteria [**CC]** for short), an international standard (ISO 15408) for the assessment and certification of the security of computer systems was created. The CC include different levels of trustworthiness (Evaluation Assurance Levels) ranging from the "EAL 1" level (functionally tested) up to "EAL 7" level (formally verified design and tested).
Creator	→ Creator of an electronic seal orr →Creator of an electronic signature
Creator of electronic seal	→Seal creator, electronic
Creator of electronic signature	→Signature creator, electronic

Cryptographic Message Syntax (CMS) RFC 5652

The Cryptographic Message Syntax (CMS) is a specification published by the Internet Engineering Task Force (IETF) that describes in ASN.1 syntax how data is protected by cryptographic measures such as digital signatures or encryption or signature data can be exchanged over the Internet.

It is based on the document originally published by RSA laboratories, PKCS#7 (Public Key Cryptography Standard) in the version 1.5, which depicts a general syntax for data to which cryptographic operations such as digital signatures or digital envelopes were applied. The PKCS#7v1.5 standard is the basis of the S/MIME protocol and the electronic signatures embedded in PDF documents and is used for the protection of the authenticity of executable software files.

The syntax is recursive so that data and envelopes can be nested or already encrypted data can be signed. Furthermore, the syntax makes it possible to authenticate additional attributes, such as time-stamps, with the data or the contents of the message and supports a number of architectures for key administration on the basis of electronic certificates.

Data

The generic term for all information that is read by electronic media, electronically processed or saved on electronic media. In information technology, data is often differentiated from document.

See also →data model.

Data Model

A data model describes the inner structures and relationship of →data among each other. As a rule, the model is described by means of a formal depiction, for example by means of a UML class diagram and an additional text description.

Deterministic Algorithm

A deterministic algorithm is an algorithm that always executes the same sequence of operations for a certain input, i.e. at every point in time, the following operation of the algorithm is defined in a definitive manner.

Digital Signature

→Signature, digital

Directory Service

A directory service is a component of a →Trust Service and is used for the publication of →certificates and certificate status information in the form of →revocation lists or →OCSP answers.

Document, Electronic

An electronic document may contain text, tables of numbers, pictures or a sequence or combination of texts, tables or pictures created or transferred in a file format by means of digitalisation (conversion into a binary code). In a broader sense, the term refers to all kinds of weakly structured or unstructured information that is available as a closed unit as a file in an IT system. (Source: Wikipedia)

DOMEA

DOMEA stands for "Document Management and Electronic Archiving in an IT-Supported Transaction" and is a concept for documentrecord management and electronic archiving in public administration. The primary goal of the DOMEA concept is the introduction of electronic folders as a further development from the "paperless office" concept from 1996. Because the same laws, rules of procedure, directives, regulations and requirements apply to electronic files than to paper files, all official business processes, workflow management and archiving shall be transferred completely into conforming IT processes. The DOMEA concept provides guidelines for this purpose, but despite its prevalence and the opportunity for certification, it is not a standard. Version 2.1 of the concept has been available since November 2005.

GERMAN Law for Implementing the "Regulation (EU) No 910/2014""	On 29.03.2017 the German parliament passed the German **"Law for Implementing the "Regulation (EU) No 910/2014""** (German word: "Gesetz zur Durchführung der eIDAS-Verordnung der EU"). The core of this omnibus law is the Trust Service Act (**[VDG]**) which facilitates the utilization of electronic trust services e.g. the digital signature. Trust Services ensure a technically high security level as well as a high probative value and enable citizens, public authorities and private companies to carry out trustworthy digital transactions in EU, EFTA or E-Government efficiently, user-friendly and paperless[99].
eIDAS-Regulation	Since 01.07.2016 trust services regarding the Regulation (EU) No 910/2014 of the European Parliament and of the council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC" **[(EU)910/2014]** can be offered in all 28 EU-member states as well as the EFTA members. The eIDAS contains Europe-wide new and mandatory rules regarding electronic identification and trust services. Trust Services contains electronic signatures, seals and timestamps but also preservation services ,e-Delivery services or website certificates. With this regulation a consistent legal framework was created for cross-border utilization of electronic identification and trust services. As an EU-regulation the eIDAS is directly applicable in all EU member states and EFTA. See → eIDAS.
Electronic Seal	→Seal, electronic
Electronic Seal, advanced	→Seal, advanced electronic
Electronic Seal, qualified	→Seal, qualified electronic
Electronic Seal creator	→Seal creator, electronic
Electronic Seal creation data	→Seal creation data, electronic
Electronic Seal creation device	→Seal creation device, electronic
Electronic Seal - Validation Data	→Seal - Validation Data, electronic
Electronic Signature	→Signature, electronic
Electronic Signature, advanced	→Signature, advanced electronic
Electronic Signature, qualified	→Signature, qualified electronic
Electronic Signature creator	→Signature creator, electronic
Electronic Signature Creation Data	→Signature creation data, electronic
Electronic Signature creation device	→Signature creation device, electronic
Electronic Signature-Validation Data	→Signature - Validation Data, electronic
Electronic Time-stamp	→time-stamp, electronic
Advanced Electronic Seal	→Seal, advanced electronic
Advanced Electronic Signature	→Signature, advanced electronic
Owner	The owner of an →archival information package is, as a rule, the client software that transferred the →archival information package to be deposited in the long-term storage through the →ArchiSafe-Module.
Evidence Record	See →Evidence Records, technical and also →**[RFC4998]** or →**[RFC6283]**.
Evidence Record Syntax	

[99] See http://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2017/20170329-zypries-digitale-signatur-spart-kosten-und-ist-sicher.html

Hash Tree

Merkle **[MER 1990]** made the suggestion to sign several sets of data with the help of a so-called authentication tree (hash tree, Merkle tree) with a single signature or time-stamp made at the root of this tree. Merkle stipulated a binary tree structure for such an authentication tree. The leaves of this tree are made of the →hash values of the information packages to be protected. Every inner node of the binary authentication tree contains one →hash value, which is generated by hashing the concatentaion of the both children nodes. The root hash value, which represents unambiguously all data objects, is signed or timestamped.. The →hash value of a certain piece of data from the total amount of data signed by this tree is saved in each leaf. The data itself is not a part of the tree; it is merely represented by its digital "fingerprints" (hash values).

The binary structure suggested by Merkle is a special case. Furthermore, authentication trees with nodes that have a maximum of k ($k > 2$) children instead of a maximum of 2 are conceivable.

Hash Function

A hash function is a cryptographic algorithm with which the (electronic) messages of any length can be mapped on a →hash value with a fixed length (e.g. 160 bit). In the case of cryptographically suitable hash functions, it is practically impossible to find two messages with the same →hash value (collision resistance) and to find a message for a given hash value that can be mapped by means of the hash function on the →hash value (one-way characteristic).

Hash Value

A hash value is a unique representation of electronic data and is also called a message digest or digital "fingerprint" of the data. A →hash function for the computation of the hash value is a function that is defined mathematically or in another way that maps input data of variable length from a pre-image (also called "universe") to output data (which is shorter as a rule) of a fixed length (the hash value) in an image. The goal is to create a "fingerprint" of the input that allows a statement about whether a certain input with all probability is identical to the original.

In the context of digital signatures (electronic signatures, seals) and time-stamps, hash values are used as unique digital representatives of the data cryptographically to be signed.

IETF

The Internet Engineering Task Force (IETF) is an open, technically oriented international association of network designers, professional users and manufacturers who concern themselves with the technical basis of the Internet and network management.

Information

Knowledge or facts that have been given "form" for acquisition, transfer, and processing, such as announcements, messages, data, or measured values. In computer science, information that is the subject of mechanical saving, processing and transmission, primarily as a sequence of characters from a certain character set (such as an alphabet) is considered.

Content Data

Content data (synonymous: primary data) is a set of information (texts, documents, processes or files or parts of a file) which is the actual goal of preservation (long-term storage).

Integrity

Electronic data have integrity if it is complete and if it can be proven that no changes or manipulations to the data can be found.

Interoperability

Interoperability in the broadest sense designates the ability of different device or software components to communicate with each other directly, i.e. in particular the ability to exchange data. In the narrower sense, interoperability is the ability of IT systems to communicate directly with other systems if they are connected through a network.

ISO 15489	ISO 15489 is an international standard. It offers guidelines for the management of the documents of public and private organisations. Key terms are 'file management', 'document management' or 'records management'. The goal of the standard is to create a framework for the management and storage of documents - regardless of their physical characteristics and their logical structure.
Canonicalisation	The canonicalisation or normalisation of an XML document describes the process of giving XML documents a unique representation (spaces, line breaks etc.). The background is the unique depiction of an XML document to the last bit so that a reproducible calculation of the →hash value is possible.
Configuration Data	Configuration data include all internal module data that is needed for the correct execution of the security-related functions, in particular the correct and reliable identification and authentication of external applications as well as of the internal modules of the archive system, and the verification and execution of archive requests.
Conformity	Conformity means the compliance of a system or component with the requirements defined for this type of system or component (system or component class).
Concatenation	Concatenation describes the process of joining two or several strings of bits or characters together and returning them as a string of bits or characters. When required, the strings of bits/characters are sorted before they are linked in order to make the reproducibility of the results possible.
Cryptographically Signed Documents	In addition to the qualified signed or sealed or timestamped documents (in the sense of **[eIDAS, Article 3(12) or 3(27) or 3(34)]**), the term "cryptographically signed documents" in this Technical Guideline also includes documents with an advanced electronic signature, seals (in the sense **[eIDAS,Article 3(11) or 3(26)]**) as well as documents with time-stamp (**[eIDAS,Article 3(33)]**) such as those often used in internal communication in or between agencies. Documents with simple signatures based on other (may be also non-cryptographic) procedures are not meant here.
Legal Person (Legal Entity)	Pursuant to (**[eIDAS]**, No. 68) “The concept of ‘legal persons’, according to the provisions of the Treaty on the Functioning of the European Union (TFEU) on establishment, leaves operators free to choose the legal form which they deem suitable for carrying out their activity. Accordingly, ‘legal persons’, within the meaning of the TFEU, means all entities constituted under, or governed by, the law of a Member State, irrespective of their legal form.”
Long-Term Archiving	See →archiving
Long-Term Storage	See →archiving
Multi-Client Capability	Information technology that can serve multiple clients, thus customers or principals, on the exact same server or the exact same software system without them having reciprocal access to their data, user administration, and the like is called multi-client capable. An IT system that has this characteristic offers the possibility of disjunct, client-oriented data storage, presentation (GUI) and configuration (customizing). Each client can only see and change their own data. (Source: Wikipedia)
Meta Data	In the broadest sense, meta data is data that describes other data. As a rule, meta data includes data that describes the structures and context of data during the processing of the data by the IT systems that create, process, administer and save the data. Meta data of an →archival information package is, as a rule, text- or XML-based meta data for the identification and reconstruction of the administrative or business context of the payload data.

Middleware

In computer science, Middleware refers to application-neutral programs that interface between applications in such a way that the complexity of these applications and their infrastructure is hidden. Middleware can also be understood as a distribution platform, i.e. as a protocol (or protocol bundle) on a higher level than regular computer communication. In contrast to the network services on a lower level that handle the simple communication between computers, Middleware supports the communication between processes. (Source: Wikipedia)

Migration

In information technology, the term migration designates the transformation of data into a different operating or storage system or into a different file format. For the trustworthy long-term storage of electronic data, it is of particular importance that the procedure shall not compromise the authenticity and integrity of the data. How this is to be accomplished is the subject of the TransiDoc project.

MoReq10

MoReq (Model Requirements for the Management of Electronic Documents and Records) is the European standard for the management of electronic records. It was developed as part of the IDA programme of the European Commission and published by the DLM Forum. Originally, MoReq should contribute to the standardisation of the exchange of documents between the European Commission and the governments of the EU member states. In the meantime, MoReq has become established as a basis of different standards for the electronic document, archive and records management. For example, the standards for the management of records in the public administration in England (TNA), in the Netherlands (ReMano), in Norway (NOARK) and in Luxembourg (SEL ECM) are based on MoReq. In contrast to other standards (such as ISO 15489), MoReq provides a very detailed list of requirements both for functional requirements for an electronic and paper-based records management system and for the associated electronic workflow management and document management systems. MoReq also includes guidelines for the consideration of operational systems and management systems and not only establishes requirements for the storage of electronic records, but also for the requirements of other electronic document-related functions such as workflow, e-mail and electronic signatures. MoReq10 is the latest and most comprehensive specification for the management of records.

Signature or Time-Stamp Renewal

The algorithms and parameters used for the digital signature or electronic time-stamps could lose their suitability as security measures as computing power increases or improved algorithms become available, which would reduce the probative value of cryptographically signed data.

Thus, § 15 of German Trust Service Act (Vertrauensdienstegesetz **[VDG, § 15]**) and **[ETSI SR 019 510], [ETSI TS 119 511]** und **[ETSI TS 119 512]** stipulates that data with a qualified electronic signature or seal or time-stamp are to be re-secured and the evidence value is to be preserved for long time "*if needed qualified signed or sealed or timestamped data shall be secured with suitable measures prior to the time at which the security value of the existing signatures, seals or time-stamps will be reduced. time-stamp"*

If there`s a compliance, business or legal need, qualified signed, sealed or timestamped documents have to be secured by appropriate measures before the security suitability of the existing signatures, seals or timestamps decreases. The new securing have to be compliant to prior art. ***[VDG § 15].***

Non-Repudiation

Non-repudiation means that the origin, sending or receipt of data and information cannot be denied.

Payload Data	Data that is transported during communication between two communication end points of an information package and does *not* contain control or log information is usually referred to as payload data. The payload data of an archival information package include→content data (synonymous: primary information), →representation information and →supplemental evidence data.
OAIS	The abbreviation "OAIS" stands for Open Archival Information System (ISO standard 14721:2012). The reason for the development of this model was the awareness that electronically archived documents may no longer be readable after a long period of time for a variety of reasons. The reference model describes an archive as an organisation in which people and systems work together in order to make archive material available to a defined group of users. However, it is not defined how an OAIS-compliant archive is to be implemented. The development of the standard was initiated by the NASA and promoted together with the European Space Agency (ESA) and space research centres in Great Britain, Canada, France, Germany, Brazil, Japan and Russia. In May 1999, the Consultative Committee for Space Data Systems (CCSDS) presented the "Reference Model for an Open Archive Information System (OAIS)" draft.
OCSP (RFC 2560 and RFC 5960)	The Online Certificate Status Protocol (OSCP) **[RFC 2560]** or. **[RFC5960]** is a protocol for requesting the status of an electronic certificate at a Trust Service Provider online.
Private Key	A private key is the part of a cryptographic pair of keys to which only the owner of the pair of keys has access. It is kept in a →personal security environment(PSE) and used in order to create →digital signatures or →electronic time-stamps or to decrypt data.
Public Key	A public key is the part of a pair of cryptographic keys that is publicly known and freely accessible. It is usually a part of a certificate and is used, beside the verification of →digital signatures or →electronic time-stamps to encrypt data for a certain person. Only this person can then decrypt the data again with the associated →private key to which only this person has access.
Public Seal - Key	A public seal – key is that part of a pair of cryptographic keys that is publicly known and freely accessible. It can be included in a certificate and is used to verify digital seals and to encrypt data. In the eIDAS regulation the public seal – key is also called →electronic seal – validation data (seee **[eIDAS, Article 3(40)]**
Public Signature - Key	A public signature key is that part of a pair of cryptographic keys that is publicly known and freely accessible. It can be included in a certificate and is used to verify electronic signatures and to encrypt data. In the eIDAS regulation the public seal – key is also called →electronic seal – validation data (seee **[eIDAS, Article 3(40)]**
Personal Security Environment (PSE)	A PSE is a storage medium for private keys and trustworthy certificates. A PSE can be realised either as a software solution, e.g. as a password-protected file in the PKCS#12 format, or as a hardware solution, e.g. in the form of a smart card (chip card).
Private Seal - Key	The private sseal – key, in **[eIDAS, Article 36]** also called electronic →seal creation data, is that part of a cryptographic pair of keys which can be used to create a seal "with a high level of confidence" (**[eIDAS, Article 36 (c)]**) under the only control of the →creator of the seal

Private Signature - Key	The private signature – key, in **[eIDAS, Article 26]** also called →signature creation data, is that part of a cryptographic pair of keys which can be used to create a signature "with a high level of confidence" (**[eIDAS, Article 26 (c)])** under the only control of the creator of the signature. It is used to sign data and decrypt encrypted data.
Log Data	Log data are log information created by a module and stored for a period of time that can be configured or added to the →archival information package.
Validation Report Data	Validation Report Data are the results of a validation check of an electronic signaturere, of an electronic seal or of an electronic time-stamp or of an Evidence Record (see →evidence record, technical) and of all related certificates, which indicate the validity of the signature, the seal or the time-stamp and the certificate concerning a defined point of time (Zeitpunkt) (normally the date and time of the signature or seal or time-stamp creation) .
Public Key Cryptography Standards (PKCS)	PKCS is a series of standards for technologies developed by the US-American company RSA Security Inc. on the basis of asymmetrical cryptographic algorithms. The most important standards in these series include: • PKCS#1: RSA Cryptography Standard, a very frequently used low-level signature format on the basis of RSA algorithm. The current version is PKCS#1, V. 2.1 **[RFC3447]**. • PKCS#7: Cryptographic Message Syntax Standard, a very widespread high-level signature format that is supported by many standard software components. The IETF's CMS specification **[RFC2630, RFC3369, RFC3852, RFC5652]** is based on this standard. • PKCS#11: Cryptographic Token Interface Standard, an application programming interface for standardised access to chip card functions. • PKCS#12: Personal Information Exchange Syntax Standard, a data format for the exchange of private keys encrypted by means of a password.
Public Key Infrastructure (PKI)	A PKI is a technical and organisational infrastructure that makes it possible to issue, distribute, manage and verify digital certificates based on asymmetrical cryptographic procedures.
Qualified Electronic Seal	→Seal, qualified electronic
Qualified Electronic Signature	→Signature, qualified electronic
Qualified Electronic Seal Creation Device	→Seal Creation Device, qualified electronic
Qualified Electronic Signature Creation Device	→Signature Creation Device, qualified electronic
Qualified Trust Service	→Trust Service, qualified
Qualified Trust Service Provider	→Trust Service Provider, qualified
Qualified Time-Stamp	→Time-Stamp, qualified
Qualified Certificate for Electronic Seals	→ Certificate for Electronic Seals, qualified
Qualified Certificate for Electronic Signatures	→ Certificate for Electronic Signatures, qualified

Relax NG	Regular Language Description for XML New Generation (RELAX NG) is a simple schema definition language for XML. A RELAX NG schema specifies samples for the structure and the content of an XML document. In doing so, a RELAX NG schema is itself an XML document, but it also offers a compact non-XML syntax. RELAX NG is described in a document of the OASIS RELAX NG Technical Committee and also as an international standard ISO/IEC 19757-2 within the Document Schema Definition Languages (DSDL). In its complexity, Relax NG is somewhere between DTD and XML schema. Compared to simple DTD, the main advantage of Relax NG is that (optionally) XML syntax can be used and unsorted contents can be supported. Furthermore, it recognises data types and name spaces. See also http://relaxng.org/.
RSA Algorithm	The RSA algorithm, which is named after its inventors (Rivest, Shamir, and Adleman), is an asymmetrical cryptographic algorithm that can be used for encryption and the creation of digital signatures. The security of this procedure is based on the assumption that the factoring problem for large numbers upon which the algorithm is based cannot be solved efficiently.
Representation Information	Information about data formats or information about software applications which were used for a machine-readable representation of the content data at the time of storage in the long-term storage.
SAGA **Standards and Architectures for E-Government Applications**	The guidelines "Standards and Architectures for E-Government Applications (SAGA)" define recommendations for the use of IT standards and IT architectures in e-government projects of the Federal Administration. The goal is to promote the interoperability, openness and scalability, reusability and investment security of e-government applications.
SASL	The *Simple Authentication and Security Layer* (SASL) is a framework that is used by different protocols for authentication. It was defined in October 1997 as **[RFC 2222]** and replaced by **[RFC4422]** in June 2006. SASL offers the application protocol a standardised possibility of negotiating communication parameters. As a rule, only an authentication method is negotiated, but it can also be agreed that an encrypted transport protocol, such as TLS, is switched to at first. The SASL implementations on both sides of the communication partners agree to a procedure which can then be used transparently by the application.
Schema, XML	A schema describes the syntactic structure of an XML file and thus defines an XML document type. XML schema (XSD) and Relax NG are common languages for the creation of schemata.
Interface	Points of connection or contact between systems or components that communicate or work with each other. IT differentiates between hardware, software and user interfaces. Software interfaces serve the exchange of applications or components amongst each other or with the operating system.
SCVP	The Server-Based Certificate Validation Protocol (SCVP) is an Internet Protocol that makes it possible for clients to outsource the creation of an X.509 certificate chain and its validation. This is needed primarily for clients that would be overloaded by the chain creation and validation due to the lack of resources or protocols. SCVP can relieve the client of all tasks (creation of the chain, checking for revocation, validation) that are part of a complete certificate verification. In contrast to →OCSP, SCVP consists of two messages: First, the client asks the server for supported validation policies that determine for which applications the server was configured. Then, the client sends the certificate IDs to the server and indicates which actions are to be carried out, which the server answers by signing them. SCVP is still fairly new and is currently supported by only a very small number of applications.

Semantics	In contrast to syntax, semantics define the meaning of the valid characters, words, and sentences in a language.
Securing Measures	Securing measures are technical and organisational measures (precautions) with the goal of ensuring the long-term and unchangeable storage of electronic documents. System-related securing measures restrict the access to the data by means of an individual configuration of the respective system or the components accessing it, e.g. by means of authorisation systems. Securing measures related to data media are storage media that rule out that information stored on them can be overwritten or changed. Document-related securing measures are those measures that are able to protect the electronic documents themselves against undetected changes and unauthorised disclosure, e.g. encryption technologies.
Seal, electronic	"'electronic seal' means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;" **[eIDAS, Article 3(25)]** In this case the →creator of an electronic seal is a legal entity.
Seal, advanced electronic	An advanced electronic seal is an →electronic seal, which meets the requirements of **[eIDAS, Article 36].** See also **[eIDAS, Article 3 No 26].**
Seal, qualified electronic	"'qualified electronic seal' means an →advanced electronic seal, which is created by a →qualified electronic seal creation device, and that is based on a →qualified certificate for electronic seal;"**[eIDAS, Article 3(27)].**
Seal creator, electronic	Pursuant to Article 3(24) in the eIDAS-Regulation **[eIDAS]**, a "creator of a seal means a legal entity who creates an electronic seal". Also see →electronic seals and →advanced electronic seals.
Seal creation data, electronic	'electronic seal creation data' means unique data, which is used by the →creator of the electronic seal to create an →electronic seal; data pursuant to **[eIDAS2, Article 3 and 36]**, with which a seal may be created, for example by a private seal key, which is connected to electronic →seal validatiaon data (public key), so that both keys form a key pair for an asymmetric cryptographic algorithm.
Seal Creation Device, electronic	Pursuant to Article 3(31) in the eIDAS-Regulation [eIDAS], an "electronic seal creation device" "means configured software or hardware used to create an →electronic seal". See also →qualified electronic seal creation device.
Seal Creation Device, qualified electronic	Pursuant to Article 3(32) in the eIDAS-Regulation **[eIDAS]**, a "qualified electronic seal creation device" "means a →electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex III " in the eIDAS-Regulation [**eIDAS].**
Seal validation data, electronic	Pursuant to Article 3(40) in the eIDAS-Regulation **[eIDAS],** an "electronic seal validation data" "means data that is used to validate an →electronic seal."
Signature, electronic	Pursuant to Article 3 (10) in the eIDAS-Regulation **[eIDAS]** electronic signature "means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the →signatory to sign" with the aim of authenticity, integrity and non-repudiation. Beside simple signatures, e.g easily forge-able bitmaps of hand written signatures, the spectrum of possible forms of electronic signatures ranges from →advanced electronic signatures pursuant to Article 3 (11) in the eIDAS-Regulation **[eIDAS]** to →qualified electronic signatures pursuant to Article 3 (12) in the eIDAS-Regulation **[eIDAS]** as a very secure form of a digital signature.

Signature, advanced electronic	Pursuant to pursuant to Article 26 in the eIDAS-Regulation **[eIDAS]**, an advanced electronic signature "shall meet the following requirements: (a) it is uniquely linked to the →signatory; (b) it is capable of identifying the signatory; (c) it is created using →electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable." An advanced electronic signature is an electronic signature with special characteristics by means of which at least a basic amount of →authenticity and →integrity can be ensured. However, unlike the →qualified electronic signature, a merely advanced electronic signature cannot replace the →written form pursuant to § 126 **[BGB]** and has less power as evidence before a court (see § 371a **[ZPO]**). Usually, one uses →digital signatures and →certificates in order to get advanced electronic signatures.
Signature, qualified electronic	Pursuant to Article 3(12) in the eIDAS-Regulation **[eIDAS]**, a "→qualified electronic signature" "means an →advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a →qualified certificate". A qualified electronic signature has the same legal effect as a hand written signature.
Signature creator, electronic	Pursuant to Article 3(13) in the eIDAS-Regulation **[eIDAS],** an "electronic signature creation data means unique data which is used by the →signatory to create an →electronic signature".
Signature Creation Data, electronic	Pursuant to Article 3(13) in the eIDAS-Regulation **[eIDAS],** an "electronic signature creation data means unique data which is used by the →signatory to create an →electronic signature".
Signature Creation Device, electronic	Pursuant to Article 3(22) in the eIDAS-Regulation **[eIDAS],** a "electronic signature creation device" "means configured software or hardware used to create an →electronic signature". See also →qualified electronic signature creation device.
Signature Creation Device, qualified electronic	Pursuant to Article 3(23) in the eIDAS-Regulation **[eIDAS]**, a "qualified electronic signature creation device" "means a →electronic signature creation device that meets the requirements laid down in Annex II " in the eIDAS-Regulation **[eIDAS].**
Signature Validation Data, electronically	Pursuant to Article 3(40) in the eIDAS-Regulation **[eIDAS],** an "→electronic signature validation data" "means data that is used to validate an →electronic signature."
Signature, digital	A digital signature is an →electronic signature or an →electronic seal based on →asymmetric cryptographic algorithms. A digital signature can only be created with the →private key (also called →signature creation data or →seal creation data) but verified by anyone using the corresponding →public key (also called →signature validation data or →seal validation data). Also see →advanced electronic signature and →qualified electronic signature or →advanced electronic seal and →qualified electronic seal.
signatory	Pursuant to Article 26 in the eIDAS-Regulation **[eIDAS],** a "signatory means a natural person who creates an →electronic signature".

Signature Verification	The signature verification includes two different verification steps. In the first step, the mathematical validity of the signature is verified to prove integrity. In the second step, the validity of the entire signature is verified with regard to the validity model on which it is based to prove authenticity. This includes the examination of whether the →certificate used for the creation of the signature is valid at the reference point in time, i.e. the time of the signature creation for a qualified electronic signature, and the current point in time for a signature used for authentication. For the validity of a certificate, it is verified whether the signature set by the issuer of the certificate is valid, whether the certificate extensions were set correctly, whether a certificate path to a trustworthy root certificate can be built and whether the certificate was not revoked.
Standard	A standard aims at standardising goods, services or processes pursuant to certain samples. In information technology, standards serve, for example, the goal of creating generally accepted and publicly accessible rules for a group of users and for a certain period of time that make it possible to use different kinds of IT systems with each other. The intention of such a standardisation is a technical or logical sample for the harmonisation of the exchange of data between IT systems with the goal of lowering the transaction costs of the data exchange processes and increasing the quality.
Syntax	The syntax defines how valid sentences are constructed in a language. Thus, a language consists of a number of valid symbols (characters, words) and a set of rules (grammar) that say how the individual characters or words are combined in order to form valid sentences. However, the syntax does not make any statement about the meaning (semantics) of the constructed sentences.
Time-Stamp Protocol	Time-Stamp Protocol is a client-server protocol standardised by the IETF in **[RFC3161]** for the issuance of time-stamps.
TransiDoc	TransiDoc (Transformation of Signed Documents) is a research project promoted by the BMWi with the goal of specifying requirements and rules (standards) for the legally viable transformation of electronically signed documents.
TR-ESOR-Middleware	The TR-ESOR-Middleware suggested as IT Reference Architecture in this Technical Guideline is a →Middleware between the client applications and the actual storage system that, above all, has functions for the long-term preservation of evidence of →cryptographically signed documents and functions for returning the supplemental evidence data (see →evidence records).
Trust Services	"Trust service" "means an electronic service normally provided for remuneration which consists of: (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time-stamps, electronic registered delivery services and certificates related to those services, or (b) the creation, verification and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those services" (see Article 3 (16) in the eIDAS-Regulation **[eIDAS]**).
Trust Service Act (German: Vertrauensdienstegesetz [VDG])	See →**"Law for Implementing the "Regulation (EU) No 910/2014""**
Trust Service Provider,	Pursuant to (**[eIDAS],** Article 3(19)) "'trust service provider' means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider;" See also →Qualified Trust Service Provider

Trust Service Provider, qualified	A qualified trust service provider means ”a →trust service provider who provides one or more →qualified trust services and is granted the qualified status by the supervisory body” (see Article 3 (20) in the eIDAS-Regulation **[eIDAS]**)
UML **Unified Modeling Language**	The Unified Modeling Language (UML) is a graphic modelling language that has been developed since the end of the 1990s for the standardised description and depiction of business processes as well as the functionality and communication of component-based IT systems. After it has been standardised by the Object Management Group (OMG), it became the worldwide standard for analysis and design notations. Since August 2003, UML has been available as UML 2 version. It is used in software engineering in the early requirement definition and system concept phases in particular and makes diagrams and notation elements available with the help of which static and dynamic aspects of any area of application can be modelled.
Binding Character	Binding character means that a legal transaction develops its intended legal effect. The prerequisite for this is, in part, compliance with the formal requirements (such as the written form) and the presence of evidence.
Availability	Electronic information is available if it can be accessed within a reasonable period of time and if it can be displayed in such a manner on the IT systems used at the time it is accessed that human users can read this information.
Validation data	See **→seal validation data, electronic or →signature validation data, electronic**
Verification Data	Verification data is data that serves to prove the correspondence of the actual characteristics with the system's, component's, data's or data group's target characteristics defined by a goal, purpose or specification. The type and scope of verification data needed to demonstrate such proof is thus always defined by goal- or purpose-based target characteristics.
Negotiability	Data / documents are "negotiable" if they (and the associated signatures and verification data) are available in formats that a typical user can read and interpret at the time of use (thus at least until the end of the retention period in this case) with typical standard IT equipment, and in doing so consistency with the original is guaranteed. Pursuant to this, a PDF/A or XML format, for example, is considered negotiable from today's perspective; a MS Word file (.doc) is not considered negotiable, though.
Confidentiality	Confidentiality means protection against unauthorised disclosure to secure personal data and operational or professional secrets. Confidentiality is the only requirement for IT security to be taken into account for the storage of electronic documents that does not arise from storage purposes, but rather from other legally protected rights to be protected.
W3C **World Wide Web Consortium**	The W3C is a scientific and business association with the goal of developing interoperable technologies to exploit the full potential of the World Wide Web. It creates its standards as recommendations and has obliged itself to solely use technologies that are free of patent fees.
X.509	**[X.509]** is an international standard format for issuing digital PKI certificates regarding the identity of the certificate owner.
Written form	
XML Extensible Markup Language	The extensible markup language (XML) is a format description language developed primarily for the Internet for the exchange of structured data and was standardised in 1997 by the Word Wide Web Consortium (W3C) (for more information, see: http://www.w3c.org/XML/).

XML Schema Definition

XML schema definition (XSD) is a recommendation of the W3C for specifying syntactic rules for the design of XML document structures. Unlike conventional XML DTD, the structure is described in the form of an XML document, i.e. in XML syntax. In addition to the definition of elements, attributes and processing instructions, XML schemata allow conditions and limitations for accessing them to be formulated.

XML Digital Signature (XML-DSig)

The XML signature specification (also referred to as XML-DSig, RFC3275) defines an XML syntax for digital signatures. It is similar to the PKCS#7 standard in its function, but it is easier to extend and specialised in signing XML documents. It is used in many advanced web standards such as SOAP, SAML or the German OSCI.

Data of any kind can be signed with XML signatures. In doing so, the XML signature can be part of the XML information package (enveloped signature), but the data can also be embedded in the XML signature itself (enveloping signature) or addressed with a URL (detached signature).

An XML signature is always assigned at least one resource, i.e. an XML tree or any binary data to which an XML link refers. In the case of an XML tree, it shall be ensured that no ambiguities arise. In order to be able to achieve this, a so-called canonicalization of the contents is necessary. Pursuant to the standard, all elements are sequenced in the order in which they arise and all attributes are arranged in alphabetical order during this process so that one longer UTF-8 string arises. Based on this, the actual hash value is then created for the signature.

Because the signature is binary character string, it cannot be embedded directly in an XML document. The binary values are coded in the Base64 format **[RFC 1521]** in order to gain ASCII readable characters from them.

In the scope of the structure of an XML document, sub-elements and the signature itself can be excluded explicitly from being signed. Conversely, any number of references can be listed that are to be signed as a single unit.

Time-Stamp, Electronic

Pursuant to Article 3(33) in the eIDAS-Regulation **[eIDAS]**, an “electronic time-stamp” “means data in →electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time”.
Often, as in the case of a →time-stamp protocol from **[RFC3161],** time-stamps are generated with the use of →digital signatures. Thus, time-stamps are electronic certification that the data signed by the time-stamp were presented at the time of the signature in the signed form.
With regard to the legal effect and admissibility as evidence in legal proceedings of time-stamps, one differentiates between simple (self-generated) time-stamps and →qualified time-stamps that were issued by →qualified trust services providers pursuant to eIDAS-Regulation **[eIDAS].**

Time-Stamp, qualified electronic

Pursuant to Article 3(34) in the eIDAS-Regulation **[eIDAS]**, a “qualified electronic time-stamp” “means an →electronic time stamp which meets the requirements laid down in Article 42 ” in the eIDAS-Regulation **[eIDAS]**.

Time-Stamp Service

A time-stamp service issues →time-stamps. Often, the →time-stamp protocol specified in IETF is used in doing so.

Time-Stamp Protocol (TSP)

TSP is a client-server protocol standardised in **[RFC3161]** by IETF for the issuance of →time-stamps.

13. Bibliography

[1999/93/EC] *Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures),* http://data.europa.eu/eli/dir/1999/93/oj, 1999

[2012/0146/COD] *European Commission. Procedure 2012/0146/COD*, http://eur-lex.europa.eu/procedure/EN/2012_146, June 2012.

[2015/1506/EU] *COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market,* http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AOJ.L_.2015.235.01.0037.01.DEU, September 2015.

[2016/679/EU] *REGULATION 2016/679/EU of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 27 April 2016* http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679

[ACMPP] Physikalisch-Technische Bundesanstalt (PTB): *Common Criteria Protection Profile for an ArchiSafe Compliant Middleware for Enabling the Legally compliant Long-Term Preservation of Electronic Documents (ACM_PP)*, respective current valid version

[AIS 20] BSI: *Anwendungshinweise und Interpretationen zum Schema (AIS), Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren*, Version 3, see https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_pdf.html

[AIS 31] BSI: *Anwendungshinweise und Interpretationen zum Schema (AIS), Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren*, Version 3, see https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_pdf.pdf?__blob=publicationFile

https://www.bsi.bund.de/cln_165/DE/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/AnwendungshinweiseundInterpretationen/anwendungshinweiseundinterpretationen_node.html - _blank

[ALGCAT] *Suitable Cryptographic Algorithms (Geeignete Kryptoalgorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 22. November 2001)*, respective current valid version, see

http://www.bundesnetzagentur.de/cln_1912/DE/Service-Funktionen/QualifizierteelektronischeSignatur/WelcheAufgabenhatdieBundesnetzagentur/GeeigneteAlgorithmenfestlegen/geeignetealgorithmenfestlegen-node.html

[ANSI X3.4] ANSI X3.4 Information Systems – *Coded Character Sets – 7-Bit American National Standard Code for Information Interchange (7-Bit ASCII)*

[ANSI X9.62] ANSI X9.62 *Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)*

[ARCHISAFE] ARCHISAFE, http://www.archisafe.de

[ArchiSig] A. Rossnagel, P. Schmücker (ed.): *Beweiskräftige elektronische Archivierung. Ergebnisse des Forschungsprojektes "ArchiSig – Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente"*, Economica Verlag, 2006

[ARO 07] A. Rossnagel, S. Fischer-Dieskau, S. Jandt, M. Knopp: *Langfristige Aufbewahrung elektronischer Dokumente*, Band 17 der Reihe "Der elektronische Rechtsverkehr", 1. Auflage, Nomos-Verlag, 2007

[ASN.1] O. Dubuisson, ASN.1 – *Communication between heterogeneous systems*, Academic Press, 2001

[BArchG] *German Federal Archiving Law (Gesetz über die Sicherung und Nutzung von Archivgut des Bundes (Bundesarchivgesetz – BArchG)* from 10.03.2017, see https://www.gesetze-im-internet.de/barchg_2017/

[BASE64] Freed, N, Borenstein, N.: *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*, section 6.8, Base64 Content-Transfer-Encoding, IETF RFC 2045, November 1996

[BDSG] *German Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG, vom 14.01.2003 (BGBl. I S. 66), last change by law from 30.06.2017 (BGBl. I S. 2097) m.W.v. 06.07.2017 ; see https://dejure.org/gesetze/BDSG 2017*

[BGB] *German Civil Code (Bürgerliches Gesetzbuch - BGB, in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Artikel 1 des Gesetzes vom 4. Juli* 2008 (BGBl. I S. 1188)); see www.gesetze-im-internet.de/bundesrecht/bgb/gesamt.pdf

[BLESS 05] Bless, R., et al.: *Sichere Netzwerkkommunikation. Grundlagen, Protokolle und Architekturen*, Springer Verlag, Berlin Heidelberg, 2005

[BORG 03] Borghoff, C., et al.: *Long-Term Preservation of Digital Documents, Principles and Practices*, Springer, 2003

[BT 01] Bröhl, G. M., Tettenborn, A., *Das neue Recht der elektronischen Signaturen*, Bundesanzeigerverlag, 2001

[C14N] *Canonical XML*, Version 1.0, W3C Recommendation, May 2001, see http://www.w3.org/TR/xml-c14n

[C14N11] *Canonical XML*, Version 1.1, W3C Recommendation, 2 May 2008, see http://www.w3.org/TR/xml-c14n11

[C14N20] *Canonical XML*, Version 2.0, W3C Recommendation, 11 April 2013, siehe unter https://www.w3.org/TR/xml-c14n2/

[CC] *Common Criteria for Information Technology Security Evaluation (CC)*, Version 3.1, see http://www.commoncriteriaportal.org

[COM(2012)238] *European Commission. Proposal for a regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market,* June 2012. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:EN:PDF

[Common-PKI] T7 e.V. and TeleTrusT e.V.: *Common PKI Specification*, Version 2.0, January 2009, see http://www.common-pki.org/uploads/media/Common-PKI_v2.0.pdf

[CRYPTO3N2] CryptoBytes, Volume 3, Number 2. *The Cryptographic Hash Function RIPEMD-160*. RSA Laboratories. Autumn 1997

[DOL02] Dollar, C. M., *Authentic Electronic Records: Strategies for Long-Term Access*, Cohasset Associates , Inc., 2002

[DSGVO] Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DSGVO)

[DSSC] T. Kunz, S. Okunick, U. Pordesch: IETF RFC5698 - *Data Structure for Security Suitabilities of Cryptographic Algorithms (DSSC)*, see http://www.ietf.org/rfc/rfc5698.txt

[EBU-BWF] European Broadcasting Union (EBU): *EBU Broadcast Wave Format – a format for audio data files in broadcasting*, Version 1, July 2001, http://tech.ebu.ch/docs/tech/tech3285.pdf

[EC14N] *Exclusive XML Canonicalization*, Version 1.0, W3C Recommendation, July 2002, see http://www.w3.org/TR/xml-exc-c14n

[eCard-1] BSI: *eCard-API-Framework – Part 1 – Overview and general definitions*, BSI TR-03112-1, Version 1.1.**2** of 27.02.2012, see https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03112/api1_teil1_pdf.pdf

[eCard-2] BSI: *eCard-API-Framework – Part 2 – eCard-Interface, BSI TR-03112-2*, Version 1.1.2 of 27.02.2012; see https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03112/api1_teil2_pdf.pdf

[eCard-3] BSI: *eCard-API-Framework – Part 3 – Management-Interface*, BSI TR-03112-3, Version 1.1.2 of 27.02.2012, see https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03112/api1_teil3_pdf.pdf

[eCard-4] BSI: *eCard-API-Framework – Part 4 – ISO24727-3-Interface*, BSI TR-03112-4 , Version 1.1.2 of 27.02.2012, see https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03112/api1_teil4_pdf.pdf

[eCard-7] BSI: *eCard-API-Framework – Part 7 – Protocols*, BSI TR-03112-7 , Version 1.1.2 of 27.02.2012, see https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03112/api1_teil7_pdf.pdf

[eGov-Org] Die Bundesregierung: *Organisationskonzept elektronsiche Verwaltungsarbeit*, see http://www.verwaltung-innovativ.de/DE/E_Government/orgkonzept_everwaltung/orgkonzept_everwaltung

[eIDAS-DG] *Gesetzes zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Durchführungsgesetz)*, Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 52, published in Bonn, 28th July 2017

[eIDAS-VO] *eIDAS (REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC)*

[ETSI EN 319 102-1 ETSI EN 319 102 – 1, *Electronic Signatures and Infrastructers (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation, V1.1.1, (2016-04), see http://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.01_60/en_31910201v010101p.pdf*

[ETSI EN 319 122-1] ETSI: *EN 319 122-1, Electronic Signatures and Infrastructers (ESI); CAdES digital signatures, Part 1: Building blocks and CAdES baseline signatures,* Version 1.1.1, see http://www.etsi.org/deliver/etsi_en/319100_319199/31912201/01.01.01_60/en_31912201v010101p.pdf

[ETSI EN 319 122-2] ETSI: *EN 319 122 – 2, Electronic Signatures and Infrastructers (ESI); CAdES digital signatures*, *Part 2: Extended CAdES signatures* , Version 1.1.1, (2016-04), see http://www.etsi.org/deliver/etsi_en/319100_319199/31912202/01.01.01_60/en_31912202v010101p.pdf

[ETSI EN 319 132-1] ETSI: *EN 319 132 – 1, Electronic Signatures and Infrastructures (ESI); XAdES digital signatures*, *Part 1: Building blocks and XAdES baseline signatures, V1.1.1, (2016-04), see http://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.01.01_60/*

[ETSI EN 319 132-2] ETSI: *EN 319 132 – 2, Electronic Signatures and Infrastructures (ESI); XAdES digital signatures*, *Part 2: Extended XAdES signatures,* V1.1.1, (2016-04), see http://www.etsi.org/deliver/etsi_en/319100_319199/31913202/01.01.01_60/en_31913202v010101p.pdf

[ETSI EN 319 142-1] ETSI *EN 319 142 – 1, Electronic Signatures and Infrastructeres (ESI); PAdES digital Signatures*, *Part 1: Building blocks and PAdES baseline signatures*, V1.1.1 (2016-04), see http://www.etsi.org/deliver/etsi_en/319100_319199/31914201/01.01.01_60/en_31914201v010101p.pdf

[ETSI EN 319 142-2] ETSI *EN 319 142 – 2, Electronic Signatures and Infrastructeres (ESI); PAdES digital Signatures*, *Part 2: Additional PAdES signatures profiles*, V1.1.1 (2016-04), see http://www.etsi.org/deliver/etsi_en/319100_319199/31914202/01.01.01_60/en_31914202v010101p.pdf

[ETSI EN 319 142-3] ETSI *EN 319 142 – 3, Electronic Signatures and Infrastructeres (ESI); PAdES digital Signatures*, *Part 3: Part 3: PAdES Document Time-stamp digital signatures* (PadES-DTS), V1.1.1 (2016-04), see http://www.etsi.org/deliver/etsi_ts/119100_119199/11914203/01.01.01_60/ts_119114203v010101p.pdf

[ETSI EN 319 162-1] ETSI *EN 319 162 – 1, Electronic Signatures and Infrastrucutres (ESI); Associated Signature Containers (ASiC)*, *Part 1: Building blocks and ASiC baseline containers*, V1.1.1 (2016-04), see http://www.etsi.org/deliver/etsi_en/319100_319199/31916201/01.01.01_60/

[ETSI EN 319 162-2] ETSI EN 319 162 – 2, *Electronic Signatures and Infrastrucutres (ESI); Associated Signature Containers (ASiC), Part 2: Additional ASiC containers,* V1.1.1 (2016-04), see https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

[ETSI EN 319 422] ETSI EN 319 422, *Electronic Signatures and Infrastrucutres (ESI); Time-stamping protocol and time-stamp token profiles,,* V1.1.1 (2016-03), see https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

[ETSI SR 019 510] ETSI SR 019 510, *Electronic Signatures and Infrastrucutres (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures,* V1.1.1 (2017-05), see https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

[ETSI TS 101 733] ETSI: TS 101 733, *Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES),* Version 2.2.1 (2013-04), see http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf

[ETSI TS 101 903] ETSI: TS 101 903, *Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)*, Version 1.4.2 (2010-12), see https://www.etsi.org/deliver/etsi_ts/101900_101999/101903

[ETSI TS 103 171] ETSI TS 103 171, *Electronic Signatures and Infrastructures (ESI)*, *XAdES Baseline Profile,* V2.1.1 (2012-03). see http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf

[ETSI TS 103 172] ETSI TS 103 172, *Electronic Signatures and Infrastructures (ESI)*, *PAdES Baseline Profile,* V2.2.2 (2013-04). see http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf

[ETSI TS 103 173] ETSI TS 103 173, *Electronic Signatures and Infrastructures (ESI)*, *CAdES Baseline Profile*, V2.2.1 (2013-04), see http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf

[ETSI TS 103 174] ETSI TS 103 174, Electronic Signatures and Infrastructures (ESI), ASiC Baseline Profile, V2.2.1 (2013-06), see http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf

[ETSI TS 119 122-3] ETSI TS 119 122 – 3*, Electronic Signatures and Infrastructers (ESI); CAdES digital signatures*, *Part 3: Incorporation of ERS mechanisms in CAdES*, V1.1.1, (2017-01), see http://www.etsi.org/deliver/etsi_ts/119100_119199/11912203/01.01.01_60/ts_119122203v010101p.pdf

[ETSI TS 119 132-3] ETSI TS 119 132 – 3*, Electronic Signatures and Infrastructures (ESI); Electronic Signatures and Infrastructures (ESI);*XAdES digital signatures; *Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in XAdES,* DRAFT, see https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

[ETSI TS 119 312] ETSI TS 119 312: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites, see https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/

[ETSI TS 119 511] ETSI TS 119 511, *Electronic Signatures and Infrastrucutres (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques,* V1.1.1, see https://www.etsi.org/deliver/etsi_ts/119500_119599/119511/01.01.01_60/ts_119511v010101p.pdf

[ETSI TS 119 512] ETSI TS 119 512, *Electronic Signatures and Infrastrucutres (ESI); Protocols for trust service providers providing long-term data preservation services,* V1.1.1, see https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

[FC 07] F. Cohen: *FastSOA*, Elsevier Inc., 2007

[FIPS180-2] United States of America National Institute for Standards and Technology (NIST): *Secure Hash Standard (SHS)*, Federal Information Processing Standard (FIPS), Publication 180-4, August 2015, siehe unter http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[GDPdU] *Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)* (BMF-Schreiben vom 16. Juli 2001 - IV D 2 - S 0316 - 136/01 -), see www.zdh.de/fileadmin/user_upload/themen/Steuerinfo/BMF-Schreiben_16-07-01_GdPDU.pdf

[GLAD 07] Gladney, H. M.: *Preserving Digital Information*, Springer Publ., 2007

[GoBD] *Grundsätze der ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD),* (BMF-Schreiben vom 14. November 2014, - IV A 4 – S 0316/13/10003 - 2014/0353090), siehe unter http://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/Datenzugriff_GDPdU/2014-11-14-GoBD.html

[GoBS] *Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)*, Schreiben des Bundesministeriums der Finanzen an die obersten Finanzbehörden der Länder vom November 1995 - IV A 8 - S 0316 - 52/95- BStBl 1995 I S. 738 see www.bundesfinanzministerium.de/

[GON 07] Gondrom, T.: *Evidence Record Syntax,* in: N. Pohlmann et al.: ISSE/SECURE 2007 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe/SECURE 2007 Conference, Vieweg + Teubner, 2007, 367 et seq.

[HGB] *German Commercial Code (Handelsgesetzbuch - HGB,* vom 10. Mai 1897, RGBl 1987, 219, zuletzt geändert durch Art. 1 G. v. 3.8.2005 I 2267); see http://bundesrecht.juris.de/bundesrecht/hgb

[HIGGINS 2010] Higgins, S.: *Standards Watch Papers ISO15498*, obtained from http://www.dcc.ac.uk/resources/briefing-papers/standards-watch-papers/iso-15489

[HK 06] Hühnlein, D., Korte, U.: *Grundlagen der elektronischen Signatur*, Bundesamt für Sicherheit in der Informationstechnik und Secu Media Verlag, Bonn / Ingelheim, 2006

[HK 06b] Hühnlein, D., Korte, U.: *Signaturformate für elektronische Rechnungen*, in Horster P. (ed.): Tagungsband "D•A•CH Security", 2006, IT-Verlag, ISBN 3-00-018166-0, 2006 Seiten 1-14, http://www.ecsec.de/pub/2006_DACH_Signaturformate.pdf

[HKS 12] Hühnlein, D., Korte, U., Schumacher, A.: *Die BSI-Richtlinien TR-ESOR und TR-RESISCAN*, in Schartner, P., Taeger, J. (ed.): "D•A•CH Security", 2012, Syssec, ISBN 978-3-00-039221-4, S. 409-420, 2012.

[HORN 04] Hornung, G.: *Der zukünftige Einsatz von Chipkarten im deutschen Gesundheitswesen*, in: Horster P. (ed.), D·A·CH Security 2004, 226

[HORN 05] Hornung, G.: *Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, Job-Card-Verfahren*, Baden-Baden, 2005

[HUE 04] Hühnlein, D.: *Intervall-Qualifizierte Zeitstempel*, in: P. Horster (ed.), Elektronische Geschäftsprozesse, S. 341, IT-Verlag, 2005, see also http://www.ecsec.de/pub/2004_EGP_IQZeitstempel.pdf

[INHE 1995] Inhester, M.: *Rechtliche Konsequenzen des Einsatzes von Bildarchivierungs- und Kommunikationssystemen (PACS)*, NJW 1995, 685

[IT-GS] BSI, *IT-Grundschutz, Die BSI-Standards – Fundament für die Informationssicherheit*, 2017, see: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

[IT-GSK-B-A] BSI, *IT-Grundschutz-Kompendium 2019, Bausteine, OPS Betrieb, OPS 1.2.2 Archivierung*, siehe auch: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_2_2_Archivierung.html

[IT-GSK-U-A] BSI, *IT-Grundschutz-Kompendium 2019, Umsetzungshinweise, OPS Betrieb, OPS 1.2.2 Archivierung*, siehe auch: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/OPS/Umsetzungshinweise_zum_Baustein_OPS_1_2_2_Archivierung.html

[ISO 13527] ISO 13527:2010, *Space data and information transfer systems -- XML formatted data unit (XFDU) structure and construction rules*, 2010

[ISO 14533-1] ISO 14533-1:2014, *Processes, data elements and documents in commerce, industry and administration – Long term signature profiles Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)*, siehe unter http://www.iso.org/, see http://www.iso.org/

[ISO 14533-2] ISO 14533-2:2012 Processes, data elements and documents in commerce, industry and administration – Long term signature profiles – Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XaDES), see http://www.iso.org/

[ISO 14533-3] ISO 14533-3:2016, *Processes, data elements and documents in commerce, industry and administration – Long term signature profiles – Part 3: Long term signature profiles for PDF Advanced Electronic Signatures (PAdES)*, see http://www.iso.org/

[ISO 14533-4] *ISO 14533-4:2019, Processes, data elements and documents in commerce, industry and administration – Part 4: Attributes pointing to (external) Proof of Existence objects used in Long term signature formats (PoEAttributes). see* ***http://www.iso.org/***

[ISO 16684-1 ISO 16684-1, *Graphic technology – Extensible metadata platform (XMP) specification – Part 1: Data model, serialization and core properties*, 2012

[ISO19005-1] ISO19005-1, *Document management — Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1)*, 2005

[ISO 19005-3] ISO 19005-3:2012: *Document management – Electronic document file format for long-term preservation – Part 3: Use of ISO 32000-1 with support for embedded files (PFD/A-3),* 2012, see http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm%3Fcsnumber%3D57229

[ISO32000-1] ISO 32000-1, *Document management — Portable document format – Part 1: PDF 1.7*, 2008

[ISO-Latin-1] ISO/IEC 8859-1:1998: *Information technology -8-bit single-byte coded graphic character sets, Part 1: Latin alphabet No. 1*, see http://www.iso.org/

[KAMPFF 97] Kampffmeyer, U., Rogalla, J.:*Grundsätze der elektronischen Archivierung,* VOI Kompendium Band 3. VOI Verband Organisations- und Informationssysteme e. V., Darmstadt 1997, ISBN 3-932898-03-6

[KNAACK 2003] Knaack, I.: *Handbuch IT-gestützte Vorgangsbearbeitung in der öffentlichen Verwaltung*, Nomos Verlag 2003

[KUSSEL 03] Kussel, S.: Die Digitalisierung der Verwaltungsgerichtsbarkeit, Berlin, 2003

[LAZ 01] Lazinger, S. S.: *Digital Preservation and Metadata*, Greenwood Publishing, 2001

[LTAP] A. Jerman Blazic, P. Sylvester, C. Wallace: *Long-term Archive Protocol (LTAP)* – draft-ietf-ltans-ltap-08, see http://tools.ietf.org/html/draft-ietf-ltans-ltap-08

[MER 1980] Merkle, R. C.: *Protocols for Public Key Cryptosystems*, Proceedings of the 1980 IEEE Symposium on Security and Privacy (Oakland, CA, USA), pages 122-134, April 1980.

[MER 1990] Merkle, R. C.: *A Certified Digital Signature*, Advances in Cryptology; CRYPTO `89, LNCS, Bd. 0435, S. 218-238, Springer Verlag, 1990

[METS] *Metadata Encoding and Transmission Standards*, see http://www.loc.gov/standards/mets/

[Moreq10] *Model Requirements for the Management of Electronic Records – Moreq10, Modular Requirements for Records Systems, Version 1.1,* ISBN: 978-92-79-18519-9, see http://www.moreq.info/index.php

[NATARCHUK2002] *Generische Anforderungen zur langzeitlichen Erhaltung elektronischer Informationen*, obtained from http://www.nationalarchives.gov.uk/documents/de_generic_requirements_vol1.pdf

[OAIS] ISO 14721:2012 Space Data and Information Transfer Systems – *Open Archival Information System (OAIS) – Reference Model. (2012)*, see http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm%3Fcsnumber%3D57284

[OASIS VR] Hühnlein, D., *OASIS DSS v1.0 Profile for Comprehensive Multi-Signature Verification Reports Version 1.0*, Committee Specification 01, 12 November 2010, see http://docs.oasis-open.org/dss-x/profiles/verificationreport/oasis-dssx-1.0-profiles-vr-cs01.pdf

[OASIS VR XSD] http://docs.oasis-open.org/dss-x/profiles/verificationreport/oasis-dssx-1.0-profiles-vr-cs01.html

[OASIS-Async] Kuehne, A.: *Asynchronous Processing Abstract Profile of the OASIS Digital Signature Services Version 1.0*, OASIS Standard, 11 April 2007, see http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-asynchronous_processing-spec-v1.0-os.pdf

[OASIS-DSS] OASIS: *Digital Signature Service Core Protocols, Elements, and Bindings, Version 1.0*, OASIS Standard, via http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.pdf

[PDF 1.4] Adobe Systems Inc.: *PDF – Reference – Third Edition – Adobe Portable Document Format Version 1.4*, Addison Wesley, ISBN 0-201-75839-3, see http://partners.adobe.com/public/developer/en/pdf/PDFReference.pdf, November 2001

[PDF 1.7] Adobe Systems Inc.: *PDF – Reference – Sixth Edition – Adobe Portable Document Format Version 1.7*, November 2006, see http://www.adobe.com/content/dam/Adobe/en/devnet/acrobat/pdfs/pdf_reference_1-7.pdf

[PDF/A-3] ISO 19005-3:2012: *Document management – Electronic document file format for long-term preservation – Part 3: Use of ISO 32000-1 with support for embedded files (PFD/A-3),* 2012, see http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm%3Fcsnumber%3D57229

[PK-DML] *Prüfkriterien für Dokumentenmanagement-Lösungen*, VOI Verband Organisations- und Informationssysteme e.V., Bonn, 2. Auflage 2004

[PKCS#12] RSA Laboratories: *PKCS#12: Personal Information Exchange Syntax Standard*, Version 1.0, June 1999, see http://www.rsa.com/

[PKCS#7] RSA Laboratories: *PKCS#7: Cryptographic Message Syntax Standard*, Version 1.5, November 1993, see http://www.rsa.com/

[PREMIS] Library of Congress: *Preservation Metadata Maintenance Activity*, see http://www.loc.gov/standards/premis/

[PTB 05] Physikalisch-Technische Bundesanstalt: *ArchiSafe-Webseite*, see http://www.archisafe.de

[RegR] *Richtlinie für das Bearbeiten und Verwalten von Schriftgut (Akten und Dokumenten) in Bundesministerien (RegR)*, see www.bmi.bund.de

[RFC1521] Borenstein, N., Freed, N.: IETF RFC 1521 – *MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies*, see http://www.ietf.org/rfc/rfc1521.txt

[RFC1945] Berners-Lee, T., Fielding, R., Frystyk, H.: IETF RFC 1945 – *Hypertext Transfer Protocol - HTTP/1.0*, see http://www.ietf.org/rfc/rfc1945.txt

[RFC2119] Bradner, S.: IETF RFC 2119 – *Key words for use in RFCs to Indicate Requirement Levels*, see http://www.ietf.org/rfc/rfc2119.txt

[RFC2401] Kent, S., Atkinson, R.: IETF RFC 2401 – *Security Architecture for the Internet Protocol (IPSec)*, see http://www.ietf.org/rfc/rfc2401.txt

[RFC2459] Housley, R., Ford, W.: IETF RFC 2459 – *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, see http://www.ietf.org/rfc/rfc2459.txt

[RFC2560] Myers, M., Ankney, A., Malpani, A, Galperin, S., Adams, C.: IETF RFC 2560 – *X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol – OCSP*, see http://www.ietf.org/rfc/rfc2560.txt

obsolete, replaced by [RFC6960]

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, P., Leach, P., Berneres-Lee, T.: IETF RFC 2616 – *Hypertext Transfer Protocol - HTTP/1.1*, see http://www.ietf.org/rfc/rfc2616.txt

[RFC2634] Hoffman, P., Editor, *Enhanced Security Services for S/MIME*, RFC 2634, June 1999, http://www.ietf.org/rfc/rfc2634.txt

[RFC3161] Adams, C., Cain, P., Pinkas, D., Zuccherrato, R.: IETF RFC 3161 – *Internet X.509 Public-Key Infrastructure – time-stamp Protocol (TSP)*, see http://www.ietf.org/rfc/rfc3161.txt

[RFC3275] Eastlake, D., Reagle, J., Solo, D.: IETF RFC 3275 – *(Extensible Markup Language) XML –Signature Syntax and Processing*, see http://www.ietf.org/rfc/rfc3275.txt

[RFC3280] Housley, R., Polk, W., Ford, W., Solo, D.: IETF RFC 3280 – *Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, see http://www.ietf.org/rfc/rfc3280.txt

obsolete, replaced by [RFC5280]

[RFC3281] Farrell, S., Housley, R.: IETF RFC3281 – *An Internet Attribute Certificate Profile for Authorization,* see http://www.ietf.org/rfc/rfc3281.txt, April 2002

obsolete, replaced by [RFC5755]

[RFC3447] Jonsson, J., Kaliski, B.: IETF RFC 3447 – *Public-Key Cryptography Standards (PKCS)#1: RSA Cryptography Specifications*, Version 2.1, see http://www.ietf.org/rfc/rfc3447.txt, 2003

[RFC3533] Pfeiffer, S.: IETF RFC 3533 – *The Ogg Encapsulation Format Version 0*, see http://www.ietf.org/rfc/rfc3533.txt, 2003

[RFC3852] Housley, R.: IETF RFC 3852 – *Cryptographic Message Syntax (CMS)*, see http://www.ietf.org/rfc/rfc3852.txt, see also RFC5652

obsolete, replaced by [RFC5652]

[RFC4346] Dierks, T., Rescorla, E.: IETF RFC 4346 - *The Transport Layer Security (TLS) Protocol*, Version 1.1, see http://www.ietf.org/rfc/rfc4346.txt

[RFC4422] Melnikov, A., Zeilenga, K.: IETF RFC 4422 – *Simple Authentication and Security Layer (SASL)*, see http://www.ietf.org/rfc/rfc4422.txt

[RFC4510] Zeilenga, K., Ed.: IETF RFC 4510 – *Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map*, see http://www.ietf.org/rfc/rfc4510.txt

[RFC4514] Zeilenga K., *Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names*, RFC 4514, June 2006, see http://www.ietf.org/rfc/rfc4514.txt

[RFC4648] Josefsson, S., SJD: IETF RFC 4510 – *The Base16, Base32, and Base64 Data Encodings*, see http://www.ietf.org/rfc/rfc4648.txt

[RFC4810] Wallace, C., Pordesch, U., Brandner, R.: IETF RFC 4810 – *Long-Term Archive Service Requirements*, see http://www.ietf.org/rfc/rfc4810.txt

[RFC4998] Gondrom, T., Brandner, R., Pordesch, U.: IETF RFC 4998 – *Evidence Record Syntax (ERS)*, see http://www.ietf.org/rfc/rfc4998.txt

[RFC5019] Deacon, A., Hurst, R.: IETF RFC5019 – *The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments*, see http://www.ietf.org/rfc/rfc5019.txt, September 2007

[RFC5035] Schaad, J., *Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility*, August 2007, see http://tools.ietf.org/html/rfc5035

[RFC5055] Freeman, T., Housley, R., Malpani, A., Cooper, D., Polk, W.: IETF RFC 5055 – *Server-Based Certification Validation Protocol*, see http://www.ietf.org/rfc/rfc5055.txt

[RFC5126] Pinkas, D.,Ross, J., and Pope, N.: IETF RFC5126– *CMS Advanced Electronic Signatures (CAdES)*, Request For Comments, http://www.ietf.org/rfc/rfc5126.txt, February 2008

[RFC5276] Wallace, C.: IETF RFC5276 – *Using the Server-Based Certificate Validation Protocol (SCVP) to Convey Long-Term Evidence Records* http://www.ietf.org/rfc/rfc5276.txt, August 2008

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., Polk, W.: IETF RFC 5280 – *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, see http://www.ietf.org/rfc/rfc5280.txt

[RFC5652] Housley, R.: IETF RFC 5652 – *Cryptographic Message Syntax (CMS)*, see http://www.ietf.org/rfc/rfc5652.txt, September 2009

[RFC5755] Farrell, S., Housley, R., Turner, S.: IETF RFC5755 – *An Internet Attribute Certificate Profile for Authorization*, http://www.ietf.org/rfc/rfc5755.txt, January 2010

[RFC5816] Santesson, S., Pope, N., *ESSCertIDv2 Update for* RFC 3161, March 2010, see http://tools.ietf.org/html/rfc5816

[RFC6283] Blazic, A. J., Saljic, S., SETCCE, Gondrom, T.: *Extensible Markup Language Evidence Record Syntax (XMLERS)*, IETF Proposed Standard , see http://tools.ietf.org/html/rfc6283, July 2011

[RFC6818] Yee, P.: *Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,* see http://tools.ietf.org/html/rfc6818, January 2013

[RFC6960] Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, C.: *X.509 Internet Public Key Infrastructure Online Certificate Status Protoccol – OCSP,* see http://tools.ietf.org/html/rfc6960, June 2013

[RoSc05] Alexander Rossnagel and Paul Schmücker (ed.): *Beweiskräftige und sichere Langzeitarchivierung elektronisch signierter Dokumente / Ergebnisse des Forschungsvorhabens ArchiSig* (Verlagsgruppe Huthig, Jehle, Rehm, 2005)

[SAGA-5] IT-Rat der Bundesregierung: SAGA 5, November 2011, see http://www.cio.bund.de/Web/DE/Architekturen-und-Standards/SAGA/saga_node.html

[SAMLv2] Cantor, S., Kemp, J., Philpott, R., Maler, E.: *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0,* OASIS Standard, 15.03.2005

[SBJ 1991] Schmidt-Beck, J. R.: *Rechtliche Aspekte der EDV-gestützten ärztlichen Dokumentation*, NJW 1991, 2335

[SBR 04] Brumme, S, Gustmann, U, Krebs, F.:*Erfolgreiche Einführung elektronischer Archive*, Deutscher Sparkassen Verlag, Stuttgart, 2004

[SCHNEIER] Schneier, B.: *Angewandte Kryptographie*, Addison-Wesley, München 1996

[SFD 06] Fischer-Dieskau, S.: *Das elektronisch signierte Dokument als Mittel zur Beweissicherung*, Band 12 der Reihe *"Der elektronische Rechtsverkehr"*, 1. Auflage 2006, Nomos-Verlag.

[SigG] *German Signature Act (Gesetz über die Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz - SigG), vom 16.5.2001, BGBl. 2001, Teil I Nr. 22, S. 876 ff., geändert durch Art 1 G v. 4.1.2005 I 2 ,* zuletzt durch Art. 4 G v. 17.07.2009)

http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/QES/Rechtsgrundlagen/SignaturGesetz16052001Id2247pdf.pdf

[SigV] *Verordnung zur elektronischen Signatur (Signaturverordnung – SigV, vom 16.11.2001, BGBl. 2001, Teil I Nr. 59, S. 3075 ff., geändert durch Art 2 G v. 4.1.2005 I 2,* zuletzt durch Art. 1 ÄndVO v. 15.11.2010)

http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/QES/Rechtsgrundlagen/SignaturVerordnungId18198pdf.pdf

[SNIA 08] SNIA - Information Management – *Extensible Access Method (XAM) – Part 1: Architecture*, Version 1.0 , Working Draft, April, 2008, see http://www.snia.org

[SOG-IS] SOG-IS Crypto Working Group: *SOG-IS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms*, see https://www.sogis.org/uk/supporting_doc_en.html

[sRGB] *Bilingual Multimedia systems and equipment - Colour measurement and management - Part 2-1: Colour management - Default RGB colour space - sRGB*, see http://www.srgb.com/srgb.html or as IEC standard: IEC 61966-2-1 – Ed. 1.0 – http://webstore.iec.ch/webstore/webstore.nsf/

http://webstore.iec.ch/webstore/webstore.nsf/artnum/025408

[TAP 03] Wallace, C., Chokani, S.: *Trusted Archive Protocol (TAP)*, Internet Draft , draft-ietf-pkix-tap-00.txt, February 2003, see http://tools.ietf.org/id/draft-ietf-pkix-tap-00.txt

[TIFF6] Adobe Systems Inc., *TIFF – Revision 6.0*, of 3 June 1992, see http://partners.adobe.com/public/developer/en/tiff/TIFF6.pdf

[TR 02102] BSI TR-02102: *Kryptographische Verfahren: Empfehlungen und Schlüssellängen*, Version 1.0, 20.06.2008

[TR 03116] BSI TR-03116: *Kryptographische Vorgaben für Projekte der Bundesregierung*

[TR-ESOR] BSI TR 03125: Preservation of Evidence of Cryptographically Signed Documents, *Main Document, V1.2.2,* this document, see also https://www.bsi.bund.de/EN/tr-esor.

[TR-ESOR-B] BSI TR 03125: Preservation of Evidence of Cryptographically Signed Documents: *Annex TR-ESOR-B: German Federal Agency Profiling, V1.2.2*

[TR-ESOR-C.1] BSI TR 03125: Preservation of Evidence of Cryptographically Signed Documents: *Annex TR-ESOR-C.1: Conformity Test Specification (Level 1 - Functional Conformity), V1.2.1*

[TR-ESOR-C.2] BSI TR 03125: Preservation of Evidence of Cryptographically Signed Documents: *Annex TR-ESOR-C.2: Conformity Test Specification (Level 2 - Technical Conformity), V1.2.1*

[TR-ESOR-C.3] BSI TR 03125: Preservation of Evidence of Cryptographically Signed Documents: *Annex TR-ESOR-C.3: Conformity Test Specification (Level 3 - Conformity with the German Federal Agency Profiling), V1.2.1*

[TR-ESOR-E] BSI TR 03125: Preservation of Evidence of Cryptographically Signed Documents: *Annex TR-ESOR-E*
Concretisation of the Interfaces on the Basis of the eCard-API-Framework, V1.2.2

[TR-ESOR-ERS] BSI TR 03125: Preservation of Evidence of Cryptographically Signed Documents: *Annex TR-ESOR-ERS Evidence Record Profiling pursuant to RFC4998 and RFC6283, V1.2.2*

[TR-ESOR-F] BSI TR 03125: Preservation of Evidence of Cryptographically Signed Documents: *Annex TR-ESOR-F Formats, V1.2.2*

[TR-ESOR-M.1] BSI TR 03125: Preservation of Evidence of Cryptographically Signed Documents: *Annex TR-ESOR-M.1 ArchiSafe-Module, V1.2.2*

[TR-ESOR-M.2] BSI TR 03125: Preservation of Evidence of Cryptographically Signed Documents: *Annex TR-ESOR-M.2 Cryptographic-Module, V1.2.2*

[TR-ESOR-M.3] BSI TR 03125: Preservation of Evidence of Cryptographically Signed Documents: *Annex TR-ESOR-M.3 ArchiSig-Module, V1.2.2*

[TR-ESOR-S] BSI TR 03125: Preservation of Evidence of Cryptographically Signed Documents: *Annex TR-ESOR-S Interface Specifications, V1.2.1, (historical)*

[TR-ESOR-VR] BSI TR 03125: Preservation of Evidence of Cryptographically Signed Documents: Annex TR-ESOR-VR: *Verification Reports for Selected Data Structures, V1.2.1*

[TR-ESOR-XBDP] BSI TR 03125: Preservation of Evidence of Cryptographically Signed Documents: Annex TR-ESOR-XBDP: *XAIP Profiling with XBARCH, XDOMEA and PREMIS, V1.2.2*

[TSP-ASS-Part1] BSI, *Criteria for Assessing Trust Service Providers against ETSI Policy Requirements, Part 1: Assessment Criteria for all TSP – ETSI EN 319 401*

[TSP-ASS-Part2] BSI, *Criteria for Assessing Trust Service Providers against ETSI Policy Requirements, Part 2: Assessment Criteria for all TSP – ETSI EN 319 511*

[TR-03138] BSI TR 03138: Ersetzendes Scannen, (RESISCAN)

[TR-03138-R] BSI TR 03138: Ersetzendes Scannen, Anlage TR 03138-R, Unverbindliche rechtliche Hinweise

[UNICODE] Unicode Consortium: *Unicode Standard* (ISBN 0-201-61633-5), see http://unicode.org/versions/Unicode4.1.0/ This is functionally equivalent to ISO/IEC 10646:2003 – *Information technology – Universal Multiple-Octet Coded Character Set (UCS)*, see http://www.iso.org/

[VDG] *Vertrauensdienstegesetz – VDG, Artikel 1 des Gesetzes zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Durchführungsgesetz)*, Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 52, published in Bonn (2017-07)

[VERS] *Victorian Electronic Records Strategy*, see http://www.prov.vic.gov.au/vers

[VOI 05] VOI – Verband Organisation und Informationssysteme e.V.: *Dokumenten-Management Vom Archiv zum Enterprise-Content-Management*, Bonn, 2005

[WSDL] W3C Recommendation: *Web Services Description Language (WSDL)* Version 1.1, see http://www.w3.org/TR/wsdl

[X.408] ITU-T: *ITU-T Recommendation X.408, Message Handling Systems: Encoded Information Type Conversion Rules*, 1988

[X.509] ITU-T: *ITU-T Recommendation X.509 (2012) - ISO/IEC 9594-8: Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks,* 2012, seehttp://www.itu.int/rec/T-REC-X.509/en

[X.680] ITU-T: *ITU-T Recommendation X.680(2002) – ISO/IEC 8824-1:2002. Information Technology – Abstract Syntax One (ASN.1): Specification of Basic Notation*, 2002

XBARCH https://www.bundesarchiv.de/fachinformationen/00895/index.html.de, Version 1.4.3

XDOMEA https://www.xrepository.de/Inhalt/urn:uuid:0e13664e-6df5-4d1f-8397-elee-d87a0d4a.xhtml, Version 2.2.0

[XFDU] Nikhinson, S., Reich, L.: *XML formatted Data Unit (XFDU), Structure and construction rules*, CCSDS 661.0-R-1, January 2007, see http://sindbad.gsfc.nasa.gov/xfdu

[XML Name] W3C: *Namespaces in XML 1.1 (Second Edition)*, W3C Recommendation 16 August 2006, see http://www.w3.org/TR/REC-xml-names/

[XML] Bray, T. et al.: *Extensible Markup Language (XML) 1.1*, second edition, W3C Recommendation, 16.August 2006, see http://www.w3.org/TR/xml

[XMLDSIG] Eastlake, D., et al.: *XML Signature Syntax and Processing (Second Edition)*, W3C Recommendation 10 June 2008 see http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/

[XMLENC] Imamura, T. et al.: *XML Encryption Syntax and Processing,* W3C Recommendation 10 December 2002 see http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/

[XMLENC 12] Imamura, T. et al.: *XML Encryption Syntax and Processing Version 1.1,* Working Draft 18 October 2012 see http://www.w3.org/TR/xmlenc-core1/

[XMLENTRUST] EnTrust XML Schema, http://www.si-tsa.gov.si/dokumenti/timestamp-protocol-20020207.xsd

[XMLERS] Blazic, A. J., Saljic, S., SETCCE, Gondrom, T.: *Extensible Markup Language Evidence Record Syntax (XMLERS)*, IETF Proposed Standard, July 2011, see http://tools.ietf.org/html/rfc6283

[XMLSACR] World Wide Web Consortium (W3C): *XML Security Algorithm Cross-Reference*. W3C Working Draft 05 January 2012, see http://www.w3.org/TR/2012/WD-xmlsec-algorithms-20120105/

[XML-SRC] World Wide Web Consortium (W3C): *XML Security Algorithm Cross-Reference*, W3C Working Group Note 11 April 2013, see http://www.w3.org/TR/xmlsec-algorithms/

[XÖV] Aktionsplan Deutschland-Online 2011, http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Projekte/Aktionsplan_2011.html

[XSD] Fallside, D. C., et al.: (ed.): *XML Schema*, W3C Recommendation, 28 October 2004, see http://www.w3.org/TR/xmlschema-0/ (Primer), see http://www.w3.org/TR/xmlschema-1/ (Structures), see http://www.w3.org/TR/xmlschema-2/ (Datatypes)

[XSD2012] W3C, *W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes*, Version 1.1, see http://www.w3.org/TR/xmlschema11-2, April 2012

[ZPO] *German Code of Civil Procedure (Zivilprozessordnung - ZPO)*, see www.gesetze-im-internet.de/zpo